(REDACTED)

FILED UNDER SEAL

EXHIBIT 6

United States District Court
Northern District of California

Valerie Torres, et al. v. Prudential Financial, Inc., et al.

Case No. 3:22-cv-07465-CRB

Expert Report of Zubair Shafiq

January 17, 2025

PROVISIONALLY FILED UNDER SEAL

(Redacted Version)

I. QUALIFICATIONS

1. I am an associate professor of computer science at the University of California-Davis, where I run a research lab focused on Internet privacy, security, and safety. My lab's research over the last several years has specifically aimed to uncover personal data collection, sharing, and usage in the online advertising ecosystem.

2. In addition to my research, I regularly teach undergraduate and graduate courses on computer networks and computer security, including special topics courses covering emerging trends in online advertising and tracking.

3. I have received several awards and distinctions for my research. I am a recipient of the Chancellor's Fellowship (2022-2023), Dean's Scholar Award (2020), National Science Foundation CAREER Award (2018), and Fitch-Beach Outstanding Graduate Research Award (2013).

4. I have co-authored more than 100 peer-reviewed research papers. I received the Best Paper Award at the 2023 ACM Internet Measurement Conference for my research on tracking, profiling, and ad targeting in the Amazon Alexa ecosystem. I also received the 2018 Andreas Pfitzmann Award at the Privacy Enhancing Technologies Symposium for my research on designing a system to reliably detect advertising and tracking information flows in mobile apps. I also received the Best Paper Award at the 2017 ACM Internet Measurement Conference for my research on identifying and investigating the abuse of a security vulnerability in Facebook Graph API. I also received the Best Paper Award at the 2012 IEEE International Conference on Network Protocols for my research on reverse-engineering proprietary network traffic protocols.

5. I am the editor-in-chief of the Proceedings on Privacy Enhancing Technologies (PoPETs). I am on the steering committee of the Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb). I am the general chair of the Workshop on Technology and Consumer Protection (ConPro). Recently, I have served as the program chair for the Workshop on Technology and Consumer Protection (ConPro 2022 and 2023) and the Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb 2022 and 2023).

6. My full qualifications are set forth in my curriculum vitae, which is attached as Appendix A. The curriculum vitae includes the list of cases in which I have submitted a report, or I have testified at trial or by deposition in the past four years. It also includes a list of publications I have authored in the past ten years.

7. I have been retained by Girard Sharp LLP as an expert in this case. I understand that Plaintiffs allege that ActiveProspect intercepted personally identifiable and sensitive information of natural persons who, while in California, visited Prudential.com, provided personal information on Prudential's form to receive a quote for life insurance, and for whom a TrustedForm Certificate URL associated with that website visit was generated from November 23, 2021 to December 13, 2022.

8. This report incorporates the opinions I offered in my June 28, 2024 expert report in support of class certification in this case.

9. I am being compensated at the rate of $500 per hour for my time. My compensation is not dependent on my conclusions or on the outcome of this action.

10. Appendix B lists the documents that I have considered and relied upon in preparing this report.

11. I reserve the right to amend, modify, or supplement my opinions as new or additional information becomes available to me in advance of trial.

II. ASSIGNMENTS

12. I was asked by the Counsel for Plaintiffs to analyze the following:

    a. Whether Prudential and Assurance IQ programmed ActiveProspect's source code on Prudential's website to intercept data submitted by Prudential website visitors and send it to ActiveProspect.

    b. Whether data in possession of Prudential, Assurance IQ, and ActiveProspect can be used to identify natural persons whose data was intercepted by ActiveProspect when they filled out a webform to request a life insurance quote on Prudential's website.

c. Whether ActiveProspect can exploit the data it intercepted through the operation of the TrustedForm software on term.prudential.com in the class period.

d. Whether ActiveProspect analyzed the contents of the data it intercepted while in transit, or while it was being sent or received, through the operation of the TrustedForm software on term.prudential.com in the class period.

e. Assertions in the Declarations of Mr. Alex Wolfe and Dr. Nathaniel Polish in support of Defendants' early summary judgment motion.

III. SUMMARY OF OPINIONS

13. Based on my analysis of the documents Prudential, Assurance IQ, and ActiveProspect have produced in discovery and in support of their early summary judgement motion, my inspection of certain databases and data that was made available by ActiveProspect and its counsel, my review of publicly available information, my own testing, and my experience, I offer the following opinions:

a. **Opinion 1**: My testing and analysis show that Prudential and Assurance IQ installed ActiveProspect's source code on its website to intercept in real time data that users input into Prudential's webform (e.g., name, email address, phone number, zip code, gender, marital status, date of birth, height, weight, medical history, medication status) and sent it to ActiveProspect. I refer to the information that users input into Prudential's webform as "user form input data" or "form input data."

b. **Opinion 2**: My testing and analysis show that data in possession of Prudential, Assurance IQ, and ActiveProspect can be used to identify natural persons whose form input data was intercepted by ActiveProspect when they filled out a webform to request a life insurance quote on Prudential's website during the Class Period.

c. **Opinion 3**: My testing and analysis show that ActiveProspect can use the form input data intercepted by TrustedForm source code on Prudential's webform during the Class Period.

d. **Opinion 4**: My testing and analysis show that ActiveProspect's TrustedForm source code analyzes the substance of the form input data as it intercepts that data from Prudential's webform and while it is in transit during the Class Period.

IV. OPINION # 1: PRUDENTIAL AND ASSURANCE IQ INSTALLED ACTIVEPROSPECT'S SOURCE CODE ON PRUDENTIAL'S WEBSITE TO INTERCEPT IN REAL TIME USER FORM INPUT DATA AND SEND IT TO ACTIVEPROSPECT

14. I understand that Prudential and its subsidiary, Assurance IQ, collaborated on the creation and maintenance of Prudential's webform at issue in this case, term.prudential.com.[1]

15. My testing and analysis of Prudential's website[2] showed that it included a section located at https://term.prudential.com/life where a person can fill a form to get an insurance quote.

16. Defendants have acknowledged,[3] and my testing confirms, that the TrustedForm script was included in the code for term.prudential.com during the class period.[4]

17. ActiveProspect explains in its End User License Agreement that TrustedForm is "intended to capture what was viewed by the site visitor on the Hosting Page, as well as the site visitor's real-time interactions with the Hosting Page, for example, clicks, mouse movements, and data inputs."[5] ActiveProspect further provides this summary of the script's functionality:

> After the TrustedForm Script is installed on the Hosting Page, when a site visitor visits the Hosting Page, the TrustedForm Script contacts the TrustedForm Server,

---

[1] Prudential's Responses to Requests for Admission No. 1 (admitting that "Assurance IQ is a wholly owned subsidiary of Prudential Financial, Inc. and that Assurance IQ, at Prudential's request, was primarily responsible for the creation and maintenance of term.prudential.com."); *id.* No. 6 (admitting that "Prudential Financial, Inc. had ultimate[] authority over term.prudential.com").

[2] It is my understanding that Prudential has now taken down the life insurance webform (https://term.prudential.com/life).

[3] Renz Dep. at 286.

[4] My initial testing of Prudential's life insurance quote webpage was conducted in November 2023, which is outside the class period. However, evidence from the Internet Archive's Wayback Machine (https://web.archive.org/web/20210401000000*/https://term.prudential.com/life) shows that the TrustedForm source code that I analyzed in November 2023 was similarly included by Prudential throughout the Class Period. The technical functionality of TrustedForm's source code, as I describe below, is the same as it was during the Class Period.

[5] AP0000039 (TrustedForm End User License Agreement last updated 4/14/2021).

> which then collects information about that site visit . . . and issues a TrustedForm Certificate. The TrustedForm Script also creates a hidden field in the Form that is used to collect and pass the TrustedForm Certificate URL.[6]

18. Below, I show how the TrustedForm software functioned on the Prudential website, which is consistent with ActiveProspect's general description of the software.

19. I describe the events that occur and are triggered by the TrustedForm script (1) when a user navigates to the webform, (2) while the user is interacting with the webform and providing form input data, and (3) when the user submits the form.

WHAT HAPPENS WHEN A USER NAVIGATES TO THE WEBFORM

20. The following figure shows the first webpage of the insurance quote form, which asks a person to tell whether they currently have life insurance.

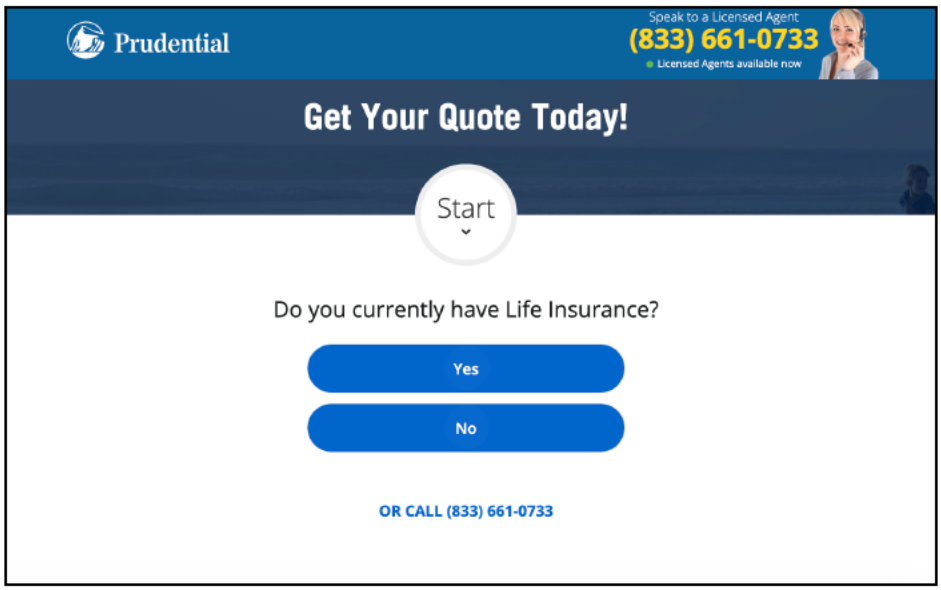


Figure: The first webpage of the life insurance quote form on Prudential's website.

21. When a website visitor navigates to the first page of the life insurance quote form, the HTML source code for this initial page has commands to include TrustedForm on the webpage as shown in the following figure. Specifically, it includes commands to:

    a. create a "trustedFormFormElement,"

[6] *Id.*

b. download the initial TrustedForm JavaScript source code,[7] and

c. check whether the user has JavaScript disabled.

Figure: Excerpt from the HTML source code for Prudential's life insurance quote webpage

22. The initial TrustedForm script (hosted by Assurance IQ on https://cdn.assurance.com) further downloads two additional JavaScript source code files from ActiveProspect, at https://cdn.trustedform.com: (1) bootstrap.js[8] and (2) trustedform-1.9.4.js.[9]

23. TrustedForm's JavaScript source code then initiates a series of more than one hundred POST[10] requests that intercept user form input data and send it to TrustedForm's server at https://api.trustedform.com/certs. ActiveProspect itself describes these POST requests as "a series of exchanges that occur in the background while the consumer has the page open."[11] I describe a few categories of POST requests below.

24. The first category of POST request transmitted to TrustedForm's server from Prudential's website contains the information necessary to set up a TrustedForm certificate ("cert"). TrustedForm defines a certificate as a "collection of all the information necessary to document a consumer's interaction with a lead generation form."[12] The payload (or

[7] https://cdn.assurance.com/insurance/public/assets/trustedForm-4a1205758bed9df95ef0ff78d02f73edd84361c32de02c6addd014f63fde670a.js

[8] https://cdn.trustedform.com/bootstrap.js?provide_referrer=false&field=xxTrustedFormCertUrl&l=1701336243713 0.2550676600214141&invert_field_sensitivity=false

[9] https://cdn.trustedform.com/trustedform-1.9.4.js

[10] A POST is typically used to upload or send data from a web browser to a web server. https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/POST.

[11] AP00000610.

[12] https://developers.activeprospect.com/docs/trustedform/getting-started/

content) of the "cert" POST request includes a JSON object,[13] which is shown in the figure below. It includes:

a. Configuration parameters of the TrustedForm certificate

b. TrustedForm version

c. Full URL of the webpage

d. Browser and screen width and height

e. User agent string containing device and operating system information. (A user agent string identifies a web browser's device and operating system).

25. There is only one "cert" POST request to TrustedForm's server, which occurs at the start of a website visitor's interaction with the first page of the webform.

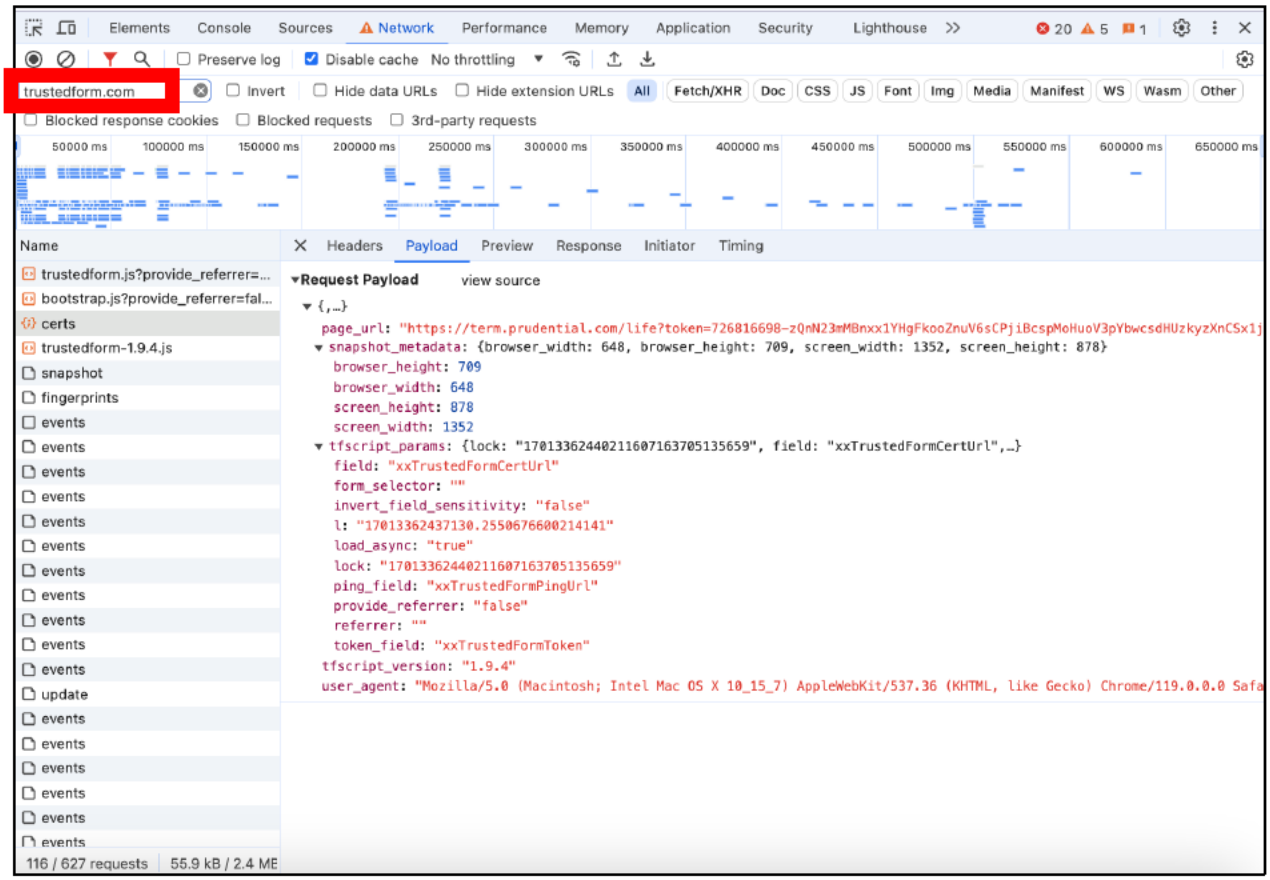


Figure: Payload of the "certs" POST request sent to TrustedForm's server

[13] JSON is a widely used way to store data in a standard human-readable text format that is also amenable to automated machine parsing. See https://developer.mozilla.org/en-US/docs/Glossary/JSON

26. The second category of POST request to TrustedForm's server includes a "snapshot" of the website's HTML. The payload of the "snapshot" POST request includes a JSON object shown in the figure below. It includes:
    a. A copy of the website's HTML's Document Object Model (DOM)[14] representation in the web browser
    b. The format in which the "snapshot" is encoded
27. The copy of the website's HTML's DOM representation[15] allows TrustedForm to re-create the webpage as it is shown in the user's web browser.
28. ActiveProspect internally describes the snapshot as "[redacted]".[16]
29. There is only one "snapshot" POST request to TrustedForm's server, which occurs at the start of a website visitor's interaction with the first page of the webform. The document "Translated Snapshot Payload" contains the decoded payload of the "snapshot" POST request and the Python script I used to this end is "Translate TrustedForm Python Script."

[14] https://developer.mozilla.org/en-US/docs/Web/API/Document_Object_Model ("The Document Object Model (DOM) connects web pages to scripts or programming languages by representing the structure of a document—such as the HTML representing a web page—in memory. Usually it refers to JavaScript, even though modeling HTML, SVG, or XML documents as objects are not part of the core JavaScript language. The DOM represents a document with a logical tree. Each branch of the tree ends in a node, and each node contains objects. DOM methods allow programmatic access to the tree. With them, you can change the document's structure, style, or content.").
[15] The DOM represents an HTML document as a tree of nodes, where each node is an object representing a part of the document (elements, attributes, text, etc.). The DOM tree nodes include all textual content in text nodes, images in .img elements, scripts as script elements, as well as visual styles of elements.
[16] AP0000392

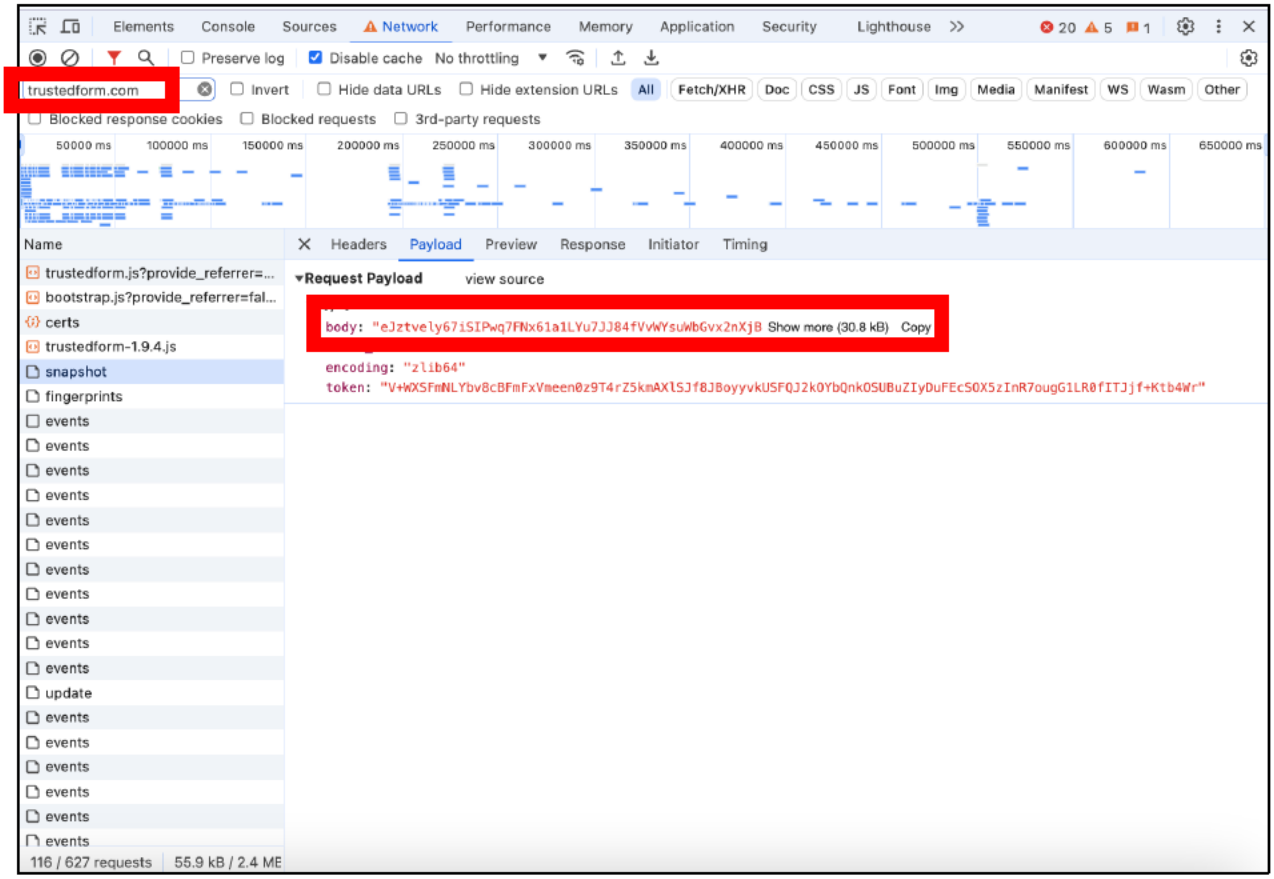


Figure: Payload of the "snapshot" POST request sent to TrustedForm's server

WHAT HAPPENS WHILE A USER INTERACTS WITH THE WEBFORM

30. The third category of POST request to TrustedForm's server includes updates about "events" on the website's HTML. The payload of the "events" POST request includes a JSON object shown in the figure below. It includes:
    a. A copy of the list of updates to the website's HTML's DOM representation in the web browser; and
    b. The format in which the "event" is encoded.
31. Unlike the first two categories of POST requests described above, which occur when the visitor first loads the webpage, the "events" requests are sent throughout the visitor's session on the webform, as each "event" occurs.
32. The vast majority of the more than one hundred POST requests sent to TrustedForm's server as a user completes the Prudential webform are "events" that are sent in real time, with frequency ranging from one second to a few seconds.

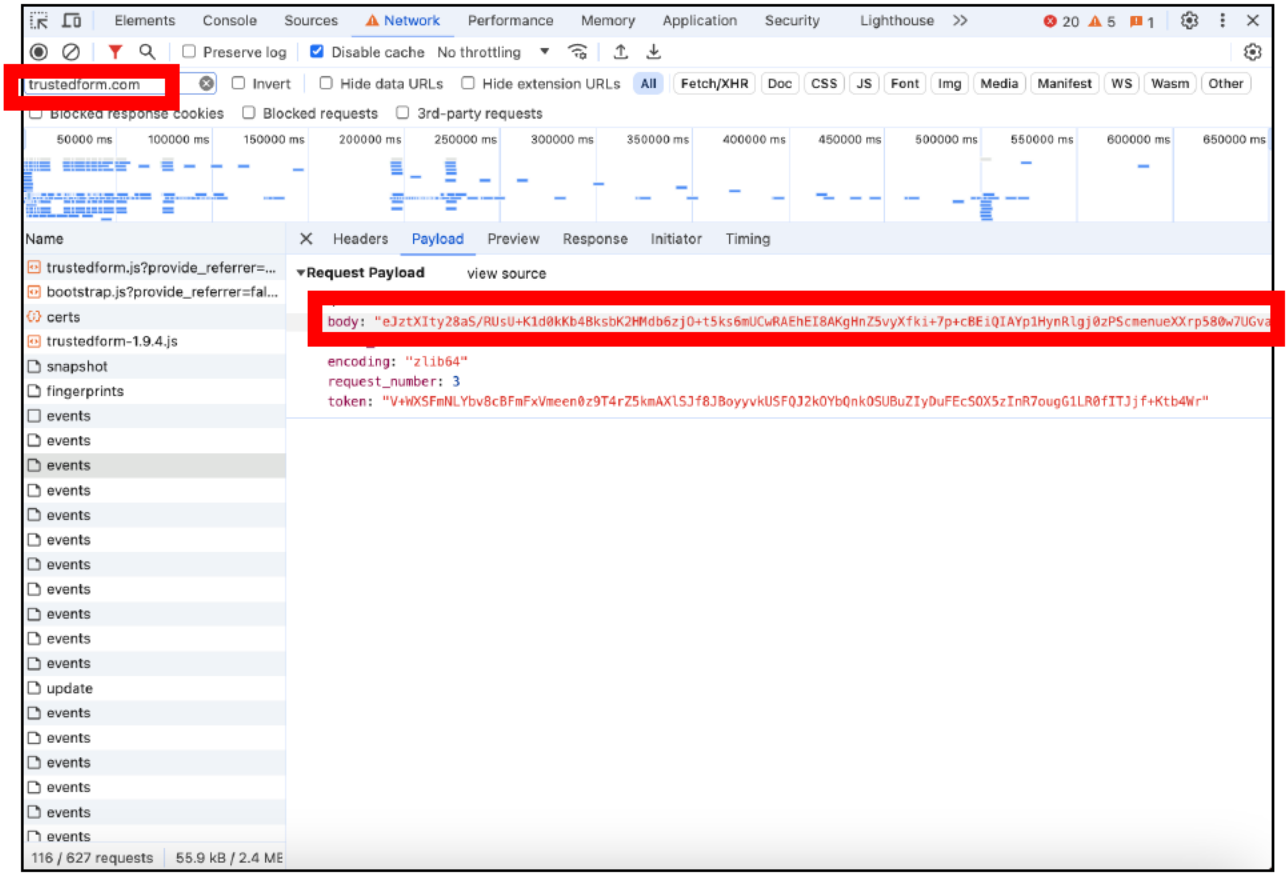


Figure: Payload of an "events" POST request sent to TrustedForm's server

33. As ActiveProspect explains on its website, recorded "events" include every time "the consumer moves or clicks their cursor or presses keys."[17]

34. Each update to the website's HTML's DOM representation allows TrustedForm to re-create the updated version of the webpage as it is currently shown in the user's web browser. In other words, the series of event updates allow TrustedForm to re-create a visual depiction of each action the user took on the webpage.

35. To collect the form data from Prudential's website and generate a replay of the user's visit to the webpage, ActiveProspect uses a technology called "event listeners,"[18] which listen

[17] AP0000610.
[18] https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener.

to various "events"[19] occurring in a user's web browser in real-time and contemporaneous with the loading of the webpage.

36. Specifically, TrustedForm's source code[20,21] [redacted]

37. [redacted] are instantaneously (i.e., in real-time and without any delay) triggered when these events occur while a user fills out different sections of the life insurance quote request form on Prudential's website.

38. ActiveProspect admits that [redacted][26]

39. ActiveProspect describes on its website that these timestamped events are bundled and sent from the user's browser to ActiveProspect's server "every few seconds" as the user continues to navigate through the webform.[27]

---

[19] https://developer.mozilla.org/en-US/docs/Web/API/Event ("An event can be triggered by the user action e.g. clicking the mouse button or tapping keyboard, or generated by APIs to represent the progress of an asynchronous task."); *id.* ("Many DOM elements can be set up to accept (or 'listen' for) these events, and execute code in response to process (or 'handle') them. Event-handlers are usually connected (or 'attached') to various HTML elements (such as <button>, , , etc.) using EventTarget.addEventListener(), and this generally replaces using the old HTML event handler attributes.").

[20] https://cdn.trustedform.com/trustedform-1.9.4.js

[21] ActiveProspect produced the non-minified version of the JavaScript source code at AP0000239

[22] https://developer.mozilla.org/en-US/docs/Web/API/Element/keydown_event ("The keydown event is fired when a key is pressed.").

[23] https://developer.mozilla.org/en-US/docs/Web/API/Element/click_event ("An element receives a click event when any of the following occurs • a pointing-device button (such as a mouse's primary button) is both pressed and released while the pointer is located inside the element. • a touch gesture is performed on the element • the Space key or Enter key is pressed while the element is focused").

[24] https://developer.mozilla.org/en-US/docs/Web/API/Document/scroll_event

[25] https://developer.mozilla.org/en-US/docs/Web/API/MutationObserver

[26] AP0000392

[27] AP0000768.

40. On term.prudential.com, the payload of "events" POST requests includes all questions on the webform and the user's answers to the questions. These questions[28] include:
    a. "Do you currently have Life Insurance?" ["Yes/No"]
    b. "What is your gender?" ["Female/Male"]
    c. "Have you used Tobacco Products within the last 12 months?" ["Yes/No"]
    d. "Are you currently married?" ["Yes/No"]
    e. "Do you have children?" ["Yes/No"]
    f. "What is your date of birth?" ["Month/DD/YYY"]
    g. "Why are you looking for life insurance?" ["Financially support loved ones/Cover debts/etc"]
    h. "What is your height?" ["ft'in""]
    i. "What is your weight?" ["Pounds"]
    j. "Are you currently taking any prescription medications?" ["Yes/No"]
    k. "In the past 5 years have you been treated or prescribed medication for any of the following conditions?" ["Anxiety / Depression / Bipolar", "Heart or circulatory disorder", "Cancer", "Respiratory disorder", "Chronic pain", "Other medical condition"]
    l. "Have you been hospitalized or missed more than 1 week of work due to anxiety, depression, or bipolar disease?" ["Yes/No"]
    m. "Are you currently employed?" ["Currently employed/Student"]
    n. "Did you have an amount of coverage in mind?" ["Over 500K"]
    o. "What is your zipcode?" ["zip"]
    p. "What is your name?" ["First Name", "Last Name"]
    q. "What is your email?" ["Email"]
    r. "Last step! Your quote is ready. Please enter your mobile number." ["Phone"]
41. The following excerpt of the payload of an "events" POST request shows that it contains the question "Are you currently married?" and the answer selected by the user. Similarly, it also shows the email address I provided on the webform in response to "What is your email?". The document "Translated Events Payload" contains the decoded payloads of all

[28] *See, e.g.*, PRU0000097.

"events" POST requests and the python script I used to this end is "Translate TrustedForm Python Script."

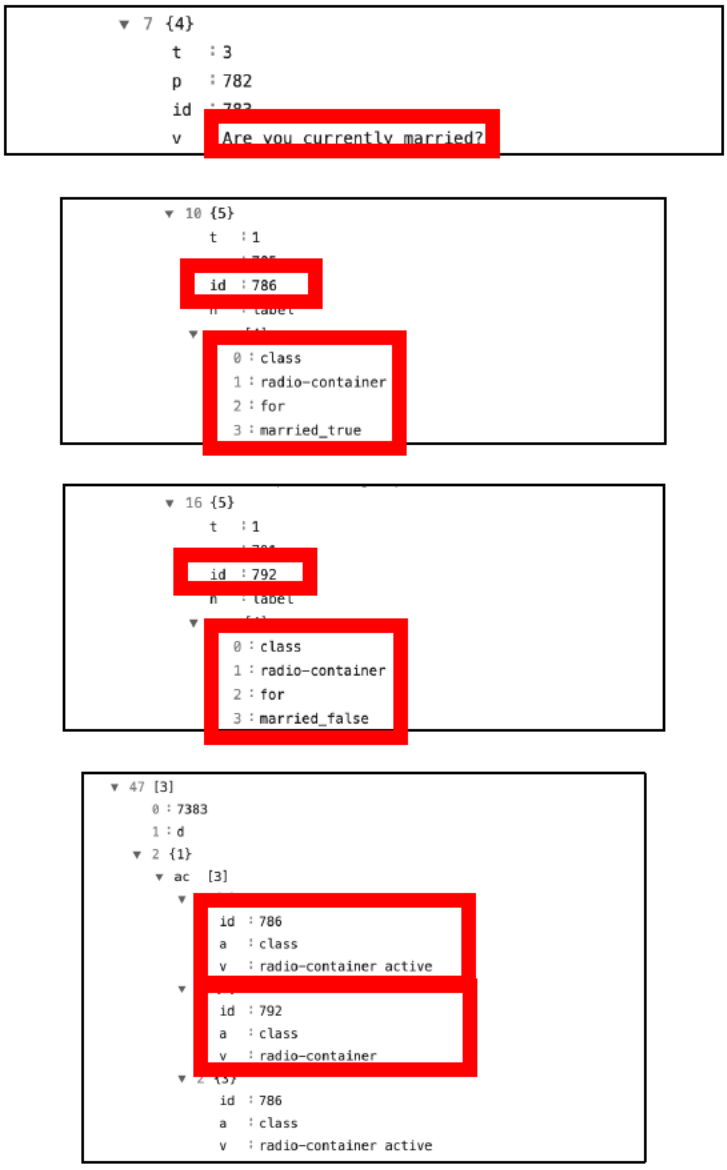


Figure: Excerpt of the decoded HTML DOM in the payload of an "events" POST request. The element ID 786 represents "married_true" and 792 represents "married_false". The user's choice is represented by the fact that the "active" radio-container is 786, not 792.

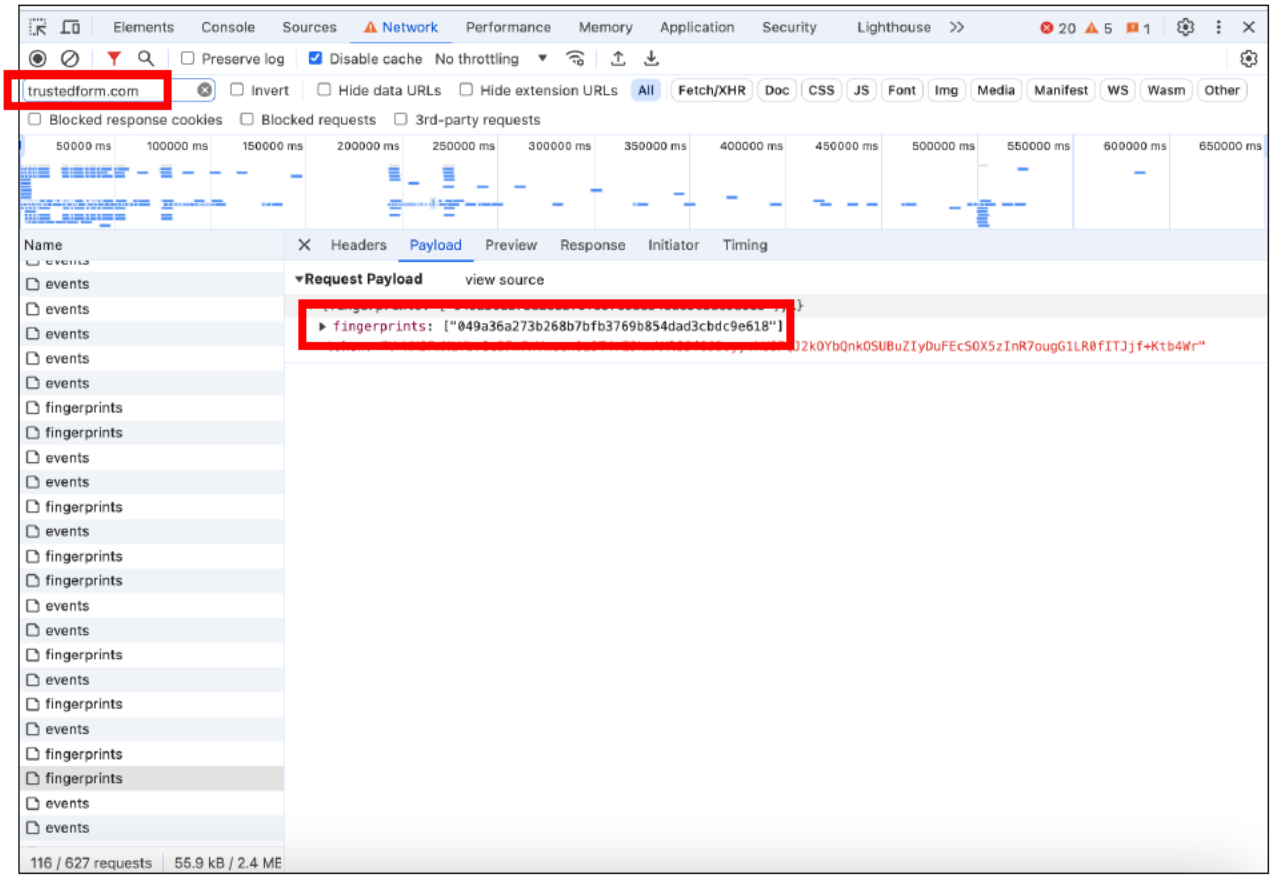
Figure: Excerpt of the decoded HTML DOM in the payload of an "events" POST request. It contains the email address I provided in plaintext.

42. The fourth category of POST request to TrustedForm's server includes a "fingerprints" POST request, which transmits the email address entered by a user in the form. The payload of the "fingerprints" POST request includes a JSON object shown in the figure below. It includes:

    s. Different hashes of email address using SHA-1[29]

43. The information sent to TrustedForm in hashed format in the "fingerprints" POST request is also sent in plaintext in the "events" POST requests. Thus, the hashed PII is duplicative of the unhashed PII.

44. The fingerprint "049a36a273b268b7bfb3769b854dad3cbdc9e618" in the figure below is the plain SHA-1 hash of the email address "zubairch@gmail.com" in the figure above.



[29] Hashing refers to a method of creating a unique digest from an input. SHA-1 is a particular method used for hashing. https://developer.mozilla.org/en-US/docs/Glossary/Cryptographic_hash_function

Figure: Payload of a "fingerprints" POST request sent to TrustedForm's server. The fingerprint "049a36a273b268b7bfb3769b854dad3cbdc9e618" is the plain SHA1 hash of the email address "zubairch@gmail.com"

45. The fifth category of POST requests to TrustedForm's server includes "updates" about user interaction on the webpage. The payload of the "updates" POST request includes a JSON object shown in the figure below. It includes:

    t. Form input method (e.g., "typing"); and

    u. typing speed in keys-per-minute and words-per-minute.

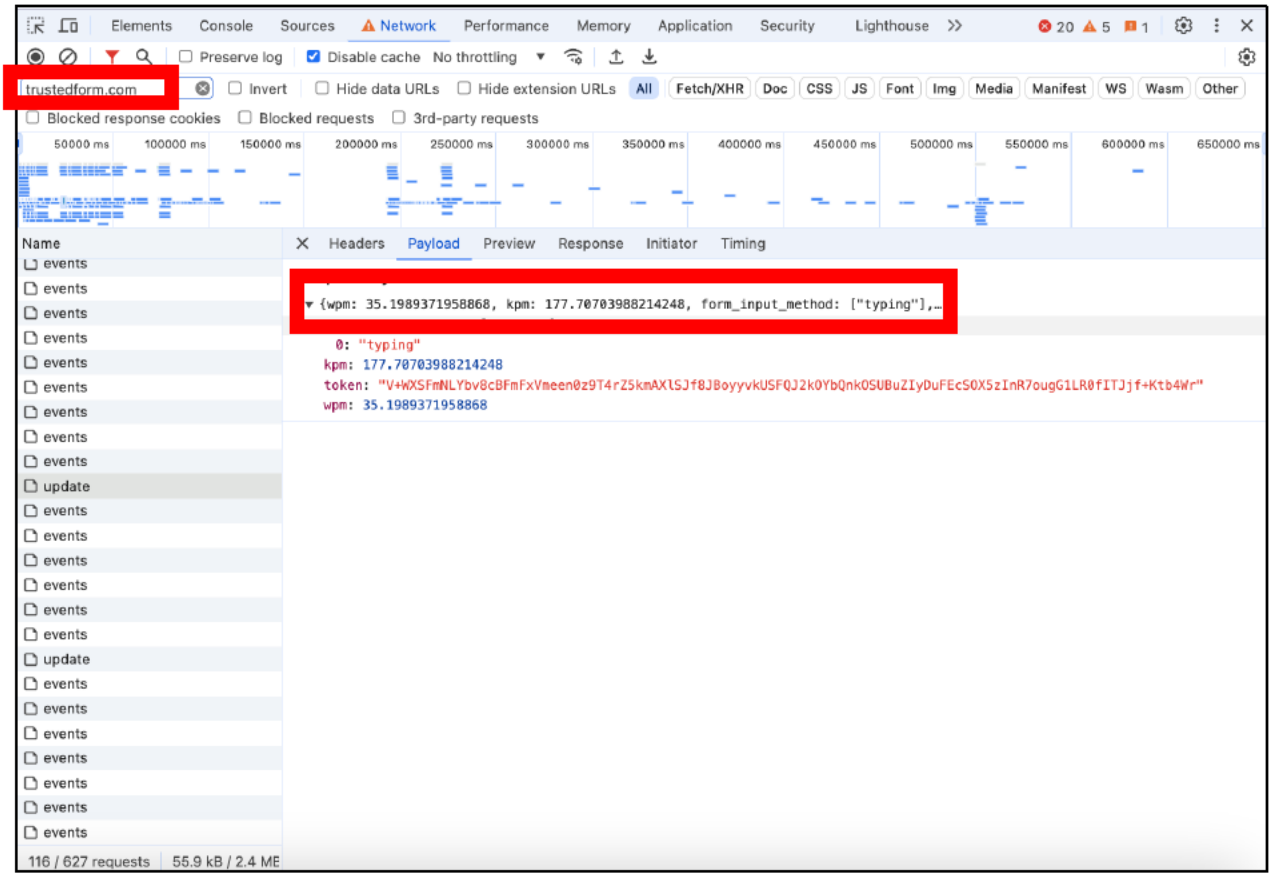


Figure: Payload of an "update" POST request sent to TrustedForm's server

WHAT HAPPENS WHEN A USER SUBMITS THE WEBFORM

46. ActiveProspect describes what happens when a user completes and submits a webform using TrustedForm as follows:

> When the consumer either abandons the page or submits a form (which also causes page abandonment) the connection between the user's browser and the TrustedForm service closes. At this point TrustedForm saves everything that the browser has sent up to it. This is the TrustedForm Certificate. It retrieves any additional files specified in the DOM from their respective servers and adds them to the Certificate, which is now complete.[30]

47. During the initial connection, the TrustedForm Script created "a hidden field in the Form that is used to collect and pass the TrustedForm Certificate URL." When a site visitor "completes the Form and submits his/her information (thereby generating a Lead), then the TrustedForm Certificate URL, within that hidden field, should be collected and sent with the rest of the Lead data."[31]

48. On term.prudential.com, Assurance IQ maintained a database that collected the information submitted by visitors to the webform.[32] [redacted][33]

BUILDING THE SESSION REPLAY VIDEO

49. All of the data shown in the preceding paragraphs is intercepted by ActiveProspect in real time and allows it to create a video recording of a user responding to each question posed by the webform on Prudential's website. For example, PRU0000097 is a video recording generated by ActiveProspect and produced by Prudential for a named plaintiff in this matter corresponding to a certificate stored by ActiveProspect.

50. The kind of tracking technology used by ActiveProspect is called session replay, which allows website developers to observe "how their page was rendered for the user and how the user interacted with their site." [34][35]

---

[30] AP0000610.
[31] *Id.*
[32] Renz Dep. at 71-72.
[33] *See, e.g.*, PRU0002712; PRU0002714 (database entries for the named plaintiffs).
[34] Acar, G., Englehardt, S. and Narayanan, A., 2020. No boundaries: data exfiltration by third parties embedded on web pages. Proceedings on Privacy Enhancing Technologies.
[35] Senol, A., Acar, G., Humbert, M. and Borgesius, F.Z., 2022. Leaky forms: A study of email and password exfiltration before form submission. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 1813-1830).

51. In fact, ActiveProspect publicly describes TrustedForm as a "session replay" technology that "documents every keystroke and every step of the consumer interaction on the page, as well as information about when and where the form was completed."[36]

52. ActiveProspect's list[37] of the data collected by TrustedForm includes

    a. "Time form was loaded by consumer",
    b. "The consumers public IP address",
    c. "Latitude and longitude based on IP location"
    d. "City based on IP location"
    e. "Country based on IP location"
    f. "Consumer User agent data, raw string"
    g. "Web address where the form was located"
    h. "Base domain address of the URL"
    i. "How form was filled (ex. Typing, autofill, or copy/paste)"
    j. "Keystrokes per minute (consumer's typing speed on form)"
    k. "Words per minute (consumer's typing speed on form)", and
    l. "View of the consumer completing the form".

53. As explained earlier, TrustedForm's source code was included on Prudential's life insurance quote request form during the class period. This means that TrustedForm's source code was loaded and ready for data collection (e.g., through the aforementioned "listeners") as soon as a user starts filling out the life insurance form.

54. The following figure plots the timeseries of the transmissions from the web browser to servers when a user fills out all sections of the form on Prudential's website. The red lines indicate the transmissions to TrustedForm's server. The blue lines indicate the transmissions from the web browser to all other servers. As this graphic demonstrates, the POST requests to TrustedForm's server occur contemporaneously as a user fills out the life insurance form on Prudential's website.

[36] https://activeprospect.com/resources/discovering-trustedform-api/
[37] https://activeprospect.com/resources/discovering-trustedform-api/

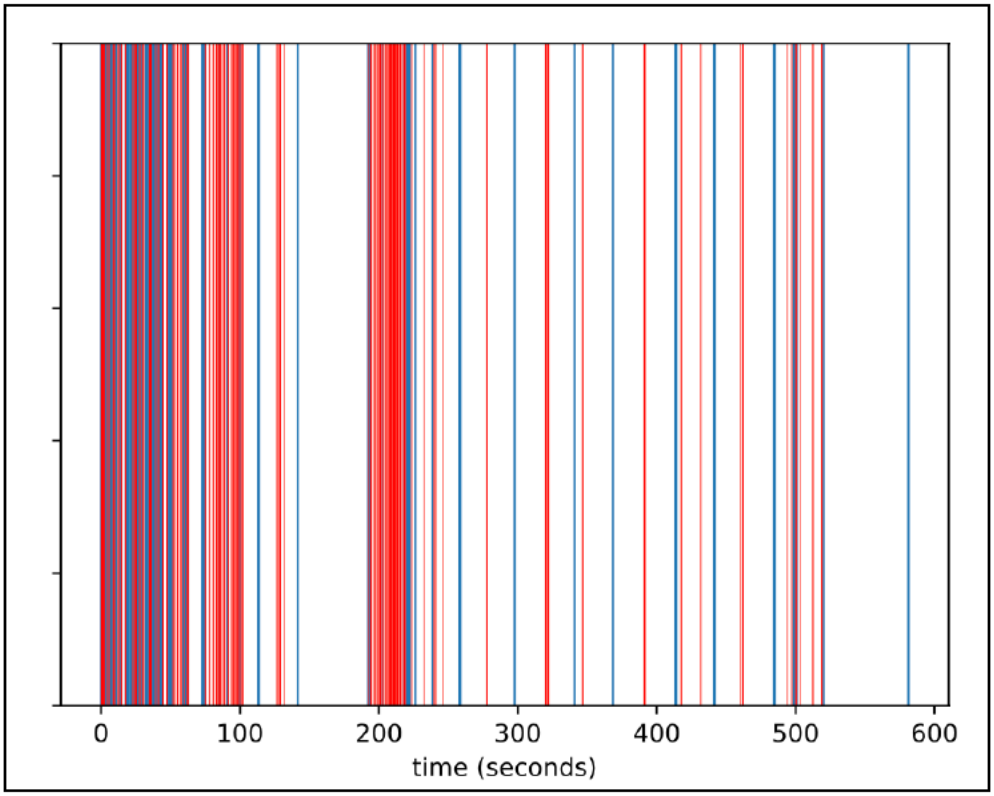


Figure: Timeseries of requests as a user fills out life insurance form on Prudential's website. The red lines represent the transmissions to TrustedForm's server.

55. Based on the foregoing, I conclude that Prudential and Assurance IQ installed ActiveProspect's source code on Prudential's website to intercept in real time user form input data (e.g., name, email address, phone number, zip code, gender, marital status, date of birth, height, weight, medical history, medication status) and sent it to ActiveProspect.

V. OPINION # 2: DATA IN POSSESSION OF PRUDENTIAL, ASSURANCE IQ, AND ACTIVEPROSPECT CAN BE USED TO IDENTIFY NATURAL PERSONS WHOSE DATA WAS INTERCEPTED BY ACTIVEPROSPECT WHEN THEY FILLED OUT A WEBFORM TO REQUEST A LIFE INSURANCE QUOTE ON PRUDENTIAL'S WEBSITE DURING THE CLASS PERIOD

56. I have been asked by Counsel to investigate whether data in possession of Prudential, Assurance IQ, and ActiveProspect can be used to identify natural persons whose data was

intercepted by ActiveProspect when they filled out a webform to request a life insurance quote on Prudential's website during the Class Period.

57. I first analyze whether a user's browser impacts the functioning of Trusted Form and whether determination of the class will be complicated by persons who block cookies, persons who disable javascript, or the presence of bots.

58. ActiveProspect's CEO testified that the operation of TrustedForm does not vary based on whether the visitor to a website is a mobile or a desktop user, what their cookie settings are, and what web browser they use. [38] This is consistent with my investigation.

TrustedForm's JavaScript Source Code is Browser Agnostic

59. To this end, I first analyze whether the interception by TrustedForm script is browser agnostic – i.e., it works the same in all major web browsers. The four major web browsers in the United States include Google Chrome, Microsoft Edge, Apple Safari, and Mozilla Firefox, which together account for more than 95% of the market share in the United States. [39,]

60. All four of these major web browsers natively support JavaScript, including the capabilities to setup "listeners"[40] and "observers".[41]

Cookie Blocking Software Does Not Impact the Functionality of TrustedForm

61. "A cookie is a small piece of information left on a visitor's computer by a website, via a web browser."[42]

62. My review of TrustedForm's JavaScript source code indicates that it does not make use of any browser cookies. This is confirmed by my observation that none of the POST

---

[38] Rafferty Dep. at 140-42.

[39] https://gs.statcounter.com/browser-market-share/all/chart.php?device=Desktop%20%26%20Mobile%20%26%20Tablet%20%26%20Console&device_hidden=desktop%2Bmobile%2Btablet%2Bconsole&multi-device=true&statType_hidden=browser&region_hidden=US&granularity=monthly&statType=Browser&region=United%20States%20of%20America&fromInt=202304&toInt=202404&fromMonthYear=2023-04&toMonthYear=2024-04&csv=1

[40] https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener#browser_compatibility

[41] https://developer.mozilla.org/en-US/docs/Web/API/MutationObserver#browser_compatibility

[42] https://developer.mozilla.org/en-US/docs/Glossary/Cookie

requests sent to TrustedForm's server include any cookies in the Cookie header.[43] Thus, I conclude that the interception by TrustedForm's JavaScript source code is not impacted by cookie blocking software.[44]

People Who Disable JavaScript Are Not Included in the Class

63. The only meaningful way to stop interception by TrustedForm's JavaScript source code is to block TrustedForm's JavaScript by disabling all JavaScript in the user's web browser settings.[45]
64. Peer-reviewed research has shown that blocking JavaScript breaks website functionality.[46] The researchers found that blocking JavaScript results in major functionality breakage on approximately two-thirds of the websites they analyzed. This is not surprising because almost all websites heavily rely on JavaScript to implement different types of functionalities.[47]
65. Thus, I conclude that a negligible fraction of users would disable JavaScript because it would prevent them from using most of the websites that exist today.
66. In any event, I understand the class to be limited to persons for whom a TrustedForm Certificate URL was generated. No TrustedForm certificate would be generated for anyone who disabled JavaScript because there would not by any POST requests to TrustedForm's server – including the "cert" POST request.
67. Thus, people who disabled JavaScript would be excluded from the class if the presence of a Trusted Form certificate is used to determine class membership.

Bots Are Unlikely to Complete the Webform and Are Excluded from the Class

68. Discovery shows that Assurance used multiple services to prevent bots[48] from filling out its forms.[49] Specifically, Kevin Bao, an Assurance IQ employee, testified that Assurance

[43] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cookie
[44] https://webkit.org/tracking-prevention/#intelligent-tracking-prevention-itp
[45] https://www.computerhope.com/issues/ch000891.htm
[46] Amjad, A.H., Shafiq, Z. and Gulzar, M.A., 2023, January. Blocking JavaScript without Breaking the Web. In Privacy Enhancing Technologies Symposium (PETS).
[47] https://almanac.httparchive.org/en/2022/javascript
[48] A bot is a computer program that can automatically interact with a webpage and do certain tasks. https://www.cloudflare.com/learning/bots/what-is-a-bot/
[49] Bao Dep. at 150-51.

69. [redacted][55]

71. It is unlikely that many, if any, bots successfully completed the webform at term.prudential.com in the class period, because of the state-of-the-art[59,60] defenses

[redacted]

described above were in place and because of the complexity and multi-page nature of the webform on term.prudential.com. Even if a bot got through a portion of the webform, it is unlikely that a bot would be able to navigate all the way to the end and submit the form in a way that it will trigger the TrustedForm script supplying a Certificate URL to Assurance's database.[61]

Records from Prudential, Assurance IQ, and ActiveProspect Can Be Used to Identify Class Members

72. Discovery shows that Prudential and Assurance IQ have a database of people who submitted the relevant webform and whose submission has a TrustedForm certificate associated with it.

73. Assurance IQ maintained a database that collected the information submitted by visitors to the webform.[62] That [redacted]

74. ActiveProspect also stores the TrustedForm certificates in its own database.[64]

75. These databases of form submissions and TrustedForm certificates can be used to reliably identify persons whose information was intercepted by ActiveProspect in California.

76. Both Assurance IQ's database and ActiveProspect's TrustedForm Certificates record the user's IP address, which identifies the user's geolocation and thus can be used to identify webform submissions that were sent from California.

[redacted]

[61] Rafferty Dep. at 130.
[62] Renz Dep. at 71-72; Bao Dep. at 65.
[63] *See, e.g.*, PRU0002712; PRU0002714 (database entries for the named plaintiffs); Bao Dep. at 65.
[64] Rafferty Dep. at 53, 77.

77. Prudential produced the session replay video for the plaintiff Valerie Torres that corresponded to the certificate ID [redacted].[65] The video included PII, such as the name, email address, and phone number, which can be used to identify a class member. The same process can be repeated for all session replay videos in Prudential's possession to identify class members.
78. In addition to reviewing the certificates themselves, any natural person who submitted Prudential's webform and whose visit was recorded by TrustedForm will have a TrustedForm Certificate URL associated with their entry in Assurance IQ's database.
79. Based on the foregoing, I conclude that the data in possession of Prudential, Assurance IQ, and ActiveProspect can be used to identify natural persons whose data was intercepted by ActiveProspect when they filled out a webform to request a life insurance quote on Prudential's website during the Class Period.

VI. OPINION 3: ACTIVEPROSPECT CAN USE THE DATA INTERCEPTED THROUGH THE OPERATION OF THE TRUSTEDFORM SOFTWARE ON PRUDENTIAL'S WEBFORM DURING THE CLASS PERIOD.

80. Discovery shows that ActiveProspect stores the intercepted user form input data, in at least two distinct databases: [redacted] Below, I describe whether ActiveProspect can use the user form input data that is stored in these two databases.
81. On December 20, 2024, I inspected ActiveProspect's databases and related data that was made available by ActiveProspect and its counsel. I inspected [redacted]

ActiveProspect Stores User Form Input Data in [redacted]

82. TrustedForm initially stores [redacted]

[65] PRU0000097
[66] Wolfe Decl. 21
[67] [redacted]

[redacted]

83. When a certificate is "claimed" by the account holder, the data is transferred from [redacted].[69] The data for class members was automatically moved from [redacted] after a very short time frame. Assurance IQ set up its account to automatically claim every certificate as soon as it was created.[70] For example, [redacted][71]

84. Mr. Wolfe provided a "representative example" of the "event data" stored in [redacted][72] I decoded this example using the "Translate TrustedForm Python Script".[73] The decoded "event data"[74] aligns with the POST request data intercepted by TrustedForm in real time, described in Section IV (Translated Events Payload).

85. Further, Mr. Wolfe confirmed that even while the data is stored in [redacted], the certificate itself and the session replay can be viewed.[75] Because the certificate uses the snapshot and events payloads to create and display the session replay video, each certificate stored [redacted] necessarily includes all the event data stored in the format needed to create the session replay.

---

[68] Wolfe Decl. 26-27
[69] Wolfe Dep. at 35:22-36:4.
[70] Renz Dep. at 154:8-17.
[71] Wolfe Dep. at 58:6-13.
[72] Wolfe Decl. 23(a)
[73] Shafiq Report Appendix B
[74] "eJxtkd1ygyAQRl+F7jWdUVONxUdxvMC/ZhsCDKxpnYzvXkw0UyfeAX s47H6UZXzkoHrgJXwbp+Uooap4mUUcWuA3kA2I8gbYgjhE4VCCAOs6i/oLOFzDzp/MD0wB 3TCeJA1+QRKYqilY84/F6p7SPEkftWO6vnivEYiYg/UzceArykEHHfZOXrrgnlHwrpmXtRlI1Er qc9h5GtUMtOitkqNgtTLNmb3hxRpHUlPBrPFIaLRgsvZGDdQVjIwVLLK/BVNdT8vyih5rVEh Bc8K27XQBoeN7z8nLPHpQ6lGM8+dE/zJMQ9yvGWpD79scV26TY7rkmMbZjvpzV73Vrszu9 8RZvj/PcnudrfoDR/Ko7g==" is decoded to "[[17,"lf",["jornaya"]],[60,"d",{"ac":[{"id":300,"a":"preping","v":"show"},{"id":300,"a":"status","v":"2"}]},[84,"d",{"r":[{"id":825}]}],[75,"d",{"a":[{"t":1,"ps":823,"id":825,"n":"iframe","a":["src","about:blank ","style","display: block !important; position: absolute; top: 0px; left: 0px; visibility: hidden;"]}]},[72,"d",{"r":[{"id":null}]}],[185,"d",{"ac":[{"id":357,"a":"preping","v":"not-show"},{"id":357,"a":"status","v":"5"}]}],[516,"d",{"ac":[{"id":397,"a":"preping","v":"show"},{"id":397 ,"a":"status","v":"2"}]}],[168,"d",{"r":[{"id":null},{"id":null}]}]]" using the standard zlib format (e.g., *see* https://en.wikipedia.org/wiki/Zlib).
[75] Wolfe Decl. 27 ("A website owner who wants to "view" an unclaimed TrustedForm Certificate is permitted to do so").

86. TrustedForm stores [redacted] ActiveProspect can decode the payloads of the POST requests (e.g., automatically using a computer program similar to the script I wrote) to extract and use the user form input data, which includes all questions on the Prudential webform and the user's answers to the questions such as medical history, medications taken, menthal health history, name, email, phone number, date of birth, gender, height, weight, etc.[76] The data would also automatically decoded when it is used to create the session replay video that can be viewed even when the data is stored in [redacted]

87. I attempted to inspect [redacted], but I was unable to do so fully. ActiveProspect did not give me the requisite permissions to run relevant queries, or view an example of data stored in the database.

88. From what I could observe without running queries on [redacted] during the inspection, [redacted], and my own testing and analysis of TrustedForm source code on Prudential's webform.

89. Mr. Wolfe states that [redacted] "remains incomprehensible unless and until it is decoded and combined with the other documents".[77] However, the data is fully comprehensible when the session replay is viewed, and Mr. Wolfe confirms certificates can be viewed before they are "claimed." In addition, my testing and analysis show that the "event data" can be readily decoded by ActiveProspect. In fact, the "event data", even individually without combining with other events, contains user form input information such as name (e.g., "Zubair"[78] "Shafiq"[79]), email address (e.g., "zubairch@gmail.com"[80]). Further, as described below, I personally

[76] Shafiq Report Para 40
[77] Wolfe Decl. 24
[78] Decoded Request Number 38
[79] Decoded Request Number 45
[80] Decoded Request Number 70

saw that [redacted][81]

ActiveProspect Stores TrustedForm Certificates in [redacted]

90. ActiveProspect stores TrustedForm certificates in [redacted]

91. Mr. Wolfe states that each TrustedForm certificate stored in [redacted] includes "the DOM, the collected events, and the 'scaffolding' necessary to show the certificate."[83]

92. I was able to inspect several certificates stored in [redacted]. For example, I inspected the certificates of plaintiffs Torres[84] and Hyman[85] [redacted]

[81] Wolfe 115:15-22 [redacted]
[82] [redacted]
[83] Wolfe Decl 29
[84] Certificate ID [redacted]
[85] Certificate ID [redacted]
[86] Shafiq Para 49
[87] Shafiq Para 42-44

93. Despite Mr. Wolfe's testimony that [redacted][88] I personally saw during the inspection that [redacted]. Mr. Wolfe was incorrect.

94. At inspection, I was able to confirm that [redacted].[89]

95. At inspection, I was able to also confirm that [redacted]

96. Further, certain ActiveProspect employees have access to client accounts, including the ability to view certificates and the session replay videos.[91] During the inspection I observed that [redacted]

[88] Wolfe 115:15-22 [redacted]

[89] I viewed [redacted] Wolfe Dep. at 134:24-135:3.

[90] https://cloud.google.com/use-cases/ocr; https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/overview-ocr

[91] AP0000761; Williams Dep. at 123:16-124:14, 124:21-126:14, 128:1-12.

97. Mr. Wolfe states that TrustedForm certificates are by default stored in the S3 Glacier "cold" storage after 30 days.[92] Mr. Wolfe further states that it can take "from three to five hours on average" to retrieve and view a certificate from S3 Glacier cold storage. Dr. Polish similarly states that "retrieving all of the stored TrustedForm Certificates from cold storage alone could take a huge number of years."[93]

98. Mr. Wolfe and Dr. Polish fail to mention that S3 provides other options to efficiently retrieve data from S3 Glacier cold storage.[94] For example,

    a. ActiveProspect can retrieve a certificate from cold storage using "expedited" retrieval that takes only "1-5 minutes".[95]

    b. ActiveProspect can also retrieve certificates en masse using "bulk" retrieval that takes "5-12 hours" to retrieve "large amounts, even petabytes of data inexpensively."[96]

99. Note that expedited and bulk retrievals are out-of-the-box options that are available to all S3 customers, including ActiveProspect, to retrieve data from S3 Glacier cold storage. ActiveProspect can readily use these two options to efficiently retrieve certificates from S3 Glacier cold storage.

100. ActiveProspect also maintains [redacted]

[92] Wolfe Decl 30
[93] Polish Decl. 89
[94] https://aws.amazon.com/s3/storage-classes/glacier/; https://docs.aws.amazon.com/AmazonS3/latest/userguide/glacier-storage-classes.html; https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects-retrieval-options.html
[95] https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects-retrieval-options.html ("**Expedited** – Quickly access your data that is stored in the S3 Glacier Flexible Retrieval storage class or S3 Intelligent-Tiering Archive Access tier. You can use this option when occasional urgent requests for a subset of archives are required. For all but the largest archived objects (250 MB+), data that is accessed by using expedited retrievals is typically made available within 1–5 minutes.")
[96] https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects-retrieval-options.html ("**Bulk** – Access your data by using the lowest-cost retrieval option in Amazon S3 Glacier. With Bulk retrievals, you can retrieve large amounts, even petabytes, of data inexpensively.")
[97] AP0000998

[redacted]

101. ActiveProspect can efficiently retrieve [redacted] using expedited or bulk retrieval options via the standard RestoreObject API call, which "Restores an archived copy of an object back into Amazon S3".[98] The "Tier" parameter simply needs be set to "Expedited" or "Bulk" to this end.

102. Note that while I observed [redacted]

103. Based on the foregoing, I conclude that ActiveProspect can use the user form input data that is intercepts through the TrustedForm source code on Prudential's website and stores in [redacted].

Mr. Wolfe and Dr. Polish's Misleading and Inaccurate Assertions

104. Regarding [redacted], Mr. Wolfe states that "None of the documents are individually comprehensible by either humans or machines. The content of an individual document appears only as a series of characters."[99] But this is wrong because, as I showed above,[100] [redacted].[101] Any human who views the certificate before it is claimed would also be able to comprehend the intercepted communications, which are displayed in the session replay video.

[98] https://docs.aws.amazon.com/AmazonS3/latest/API/API_RestoreObject.html
[99] Wolfe Decl. 23
[100] Para 82
[101] Wolfe Decl 27.

105. Mr. Wolfe states that "The TrustedForm Certificate URL is essential to locate and retrieve the associated TrustedForm Certificate. ActiveProspect does not maintain any index that links TrustedForm Certificate URLs with the underlying website visits to which those Certificate URLs correspond."[102] This is incorrect. ActiveProspect maintains [redacted]

106. Mr. Wolfe states that "ActiveProspect has no practical way to locate the TrustedForm Certificate for a specific Assurance IQ website visit without the associated TrustedForm Certificate URL, which is stored by Assurance IQ alongside the associated user record."[105] This is also contradicted by the fact that [redacted]

107. Mr. Wolfe [redacted]

[102] Wolfe Decl. 39
[103] Para 95
[104] Wolfe Dep. at 170:9-22 [redacted]
Id. at 170:23-171:13 [redacted]
[105] Wolfe Decl. 42
[106] Wolfe Dep. at 158:18-160:15.
[107] *Id.*

[redacted]

108. Regarding cold storage, Mr. Wolfe states that "ActiveProspect would need to retrieve each TrustedForm Certificate from cold storage—a process that can take from 3–5 hours per Certificate—and then download, decompress, and view each individual Certificate in order to try to obtain this information."[108] He goes on to state that "ActiveProspect also has no mechanism to download, decompress, process, and save each of the individual TrustedForm Certificates in bulk."[109] He also states that "Any effort to access or retrieve TrustedForm Certificates or user form inputs another way would require ActiveProspect to fundamentally redesign the TrustedForm system from the ground up. This would be an extremely challenging, time-consuming, and expensive task."[110] This is misleading and wrong because (1) TrustedForm already stores and can access certificate information, which include user form inputs, in "hot" storage of [redacted] for at least a month after they are created by default; and (2) ActiveProspect can readily use expedited and bulk retrieval out-of-the-box options provided by S3 Glacier to retrieve certificates stored in cold storage.

109. Mr. Wolfe also describes the use of encryption by ActiveProspect: (1) to encrypt the payloads of POST requests, containing intercepted user form input data, sent by TrustedForm's JavaScript source code to TrustedForm server[111] and (2) to encrypt certificate data stored [redacted][112] and [redacted].[113] It is noteworthy that none of these two types of encryption protects user form input or certificate data from

---

[108] Wolfe Decl. 39
[109] Wolfe Decl. 41
[110] Wolfe Decl. 43
[111] Wolfe Decl. 17 ("After TrustedForm's event listeners pick up each "event" on a webform, TrustedForm collects the data behind the event and then timestamps, batches, and compresses the events and sends them to ActiveProspect's server in "bundles" via a series of encrypted POST requests.")
[112] Wolfe Decl. 21 ("The event data remains fully encrypted at rest in [redacted].")
[113] Wolfe Decl. 28 ("If a website owner "claims" a Certificate generated on its website, [redacted])

ActiveProspect itself. Regarding the former, Mr. Wolfe confirmed at his deposition that [redacted],[114] which is used to protect data from a man-in-the-middle (MITM) attacks from a third-party like an Internet Service Provider -- not from ActiveProspect itself. This encryption is applied after interception by TrustedForm's JavaScript source code. TrustedForm's server automatically decrypts the encrypted POST payload data that is sent by TrustedForm's JavaScript source code as part of ActiveProspect receiving the transmission—before the data has come to rest. Regarding the latter, Mr. Wolfe confirmed at his deposition that [redacted],[115] which is mainly used to protect data in case of a data breach at Amazon -- not from ActiveProspect itself. This is also consistent with ActiveProspect's interrogatory response to how it encrypts TrustedForm certificates and any related data.[116] Simply put, both types of encryption are transparent to ActiveProspect, which has access to plain or decrypted user form input or certificate data.

110. I further inspected TrustedForm's server-side source code to confirm [redacted].[119]

[114] Wolfe Dep. 111:1-14; 206: 6-13; 209:1-7
[115] Wolfe Dep. 110:12-16; 207:18-23
[116] Defendant ActiveProspect, Inc.'s Responses and Objections to Plaintiffs' Fourth Set of Interrogatories. Response to Interrogatory No. 9. December 13, 2024.
[117] AP_SCODE0000011-AP_SCODE0000014; AP_SCODE0000015-AP_SCODE0000016
[118] Wolfe Dep. Ex. 142 (https://community.activeprospect.com/posts/4766190-trustedform-lead-matching) ("Beginning July 5, 2023 TrustedForm certificates began hiding all form input data in session replays until lead matching is performed if a lead's email address or phone number is recorded by the certificate as part of our new Enhanced PII Protection.")
[119] Wolfe Dep. 127:1-25; 128:1-22

VII. OPINION 4: ACTIVEPROSPECT ANALYZED THE SUBSTANCE OF THE DATA AS IT INTERCEPTED THAT DATA FROM TERM.PRUDENTIAL.COM THROUGH THE OPERATION OF THE TRUSTEDFORM SOFTWARE DURING THE CLASS PERIOD.

111. Recall from above that [redacted]

[120] https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener.

[121] https://developer.mozilla.org/en-US/docs/Web/API/Event ("An event can be triggered by the user action e.g. clicking the mouse button or tapping keyboard, or generated by APIs to represent the progress of an asynchronous task."); *id.* ("Many DOM elements can be set up to accept (or 'listen' for) these events, and execute code in response to process (or 'handle') them. Event-handlers are usually connected (or 'attached') to various HTML elements (such as <button>, , , etc.) using EventTarget.addEventListener(), and this generally replaces using the old HTML event handler attributes.").

[122] https://cdn.trustedform.com/trustedform-1.9.4.js

[123] ActiveProspect produced the non-minified version of the JavaScript source code at AP0000239

[124] AP0000907 - AP0000922

[125] https://developer.mozilla.org/en-US/docs/Web/API/Element/keydown_event ("The keydown event is fired when a key is pressed.").

[126] https://developer.mozilla.org/en-US/docs/Web/API/Element/click_event ("An element receives a click event when any of the following occurs • a pointing-device button (such as a mouse's primary button) is both pressed and released while the pointer is located inside the element. • a touch gesture is performed on the element • the Space key or Enter key is pressed while the element is focused").

[127] https://developer.mozilla.org/en-US/docs/Web/API/Document/scroll_event

[128] https://developer.mozilla.org/en-US/docs/Web/API/MutationObserver

[redacted]. TrustedForm's source code then contemporaneously sends the intercepted user form input information to TrustedForm's server. Thus, ActiveProspect actively analyzes the form data input by users in real time and contemporaneously sends the information to TrustedForm's server.

Dr. Polish's Misleading and Inaccurate Assertions

112. Dr. Polish states that "The "contents or meaning" of a user's webform inputs are not transmitted over the Internet through the use of TrustedForm."[132] This statement is incorrect. The contents and meaning of user form input data is transmitted over the Internet in the payloads of POST requests. The "Translated Events Payload" file that contains the payloads of POST requests shows that it includes the content of user form input data such as name (e.g., "Zubair"[133] "Shafiq"[134]), email address (e.g., "zubairch@gmail.com"[135]). As discussed below in more detail, for each form field on term.prudential.com, the POST request for the final keystroke in that field includes not only the key that was pressed, but then entirety of what was typed into that field. Similarly, [redacted]

129 [redacted]

130 [redacted]

131 [redacted]

[132] Polish Decl. 103
[133] Decoded Request Number 38
[134] Decoded Request Number 45
[135] Decoded Request Number 70

113. Dr. Polish states that "The TrustedForm JavaScript does not at any point attempt to decipher the "events" to try to glean the meaning of any website visitor's communications."[136] This statement is incorrect. My analysis of the TrustedForm's JavaScript source code[137] shows [redacted]

114. Dr. Polish states that "I have reviewed the report of Plaintiffs' expert, Dr. Zubair Shafiq, in support of Plaintiffs' Motion for Class Certification. In that report, Dr. Shafiq described using several programs to decode, concatenate, and translate into a readable 'payload' the more than 100 POST requests containing the encoded events that TrustedForm collected during his visit to the Prudential website in June 2024. From my

[136] Polish Decl. 115
[137] AP0000907-- AP0000922
[138] *See also* Wolfe Dep. Ex. 142 (AP website post describing the Lead Matching feature: "TrustedForm Certify runs in the background to create a TrustedForm certificate and begins checking for any e-mail addresses or phone numbers. Regular expressions are used to search the source code and user interactions for patterns that match contact information.").

review of Dr. Shafiq's report, it appears that he performed this analysis only after all of the events had arrived at their intended destination. By definition, those events and the data encoded in the POST requests were not 'in transit' when Dr. Shafiq performed these operations."[139] He goes on to state that "I understand the question in this case is whether ActiveProspect 'read or attempted to read, or to learn the contents or meaning of,' Plaintiffs' communications while they were 'in transit.' The fact that Dr. Shafiq decoded the events in more than 100 encrypted POST requests, put those decoded events together, and created and ran a program to interpret and translate the 3 combined events into readable form after they were no longer 'in transit,' does not show that ActiveProspect could do, or did, the same thing at any point in time, including when those events were 'in transit.'"[140] The assertion that decoding the event data only happens after the data is no longer "in transit" is incorrect and misleading.

115. Dr. Polish misses a key point here. TrustedForm's client-side source code intercepts the event data "in the plain," or in plaintext ***before*** it is encoded and sent to TrustedForm's server in POST request payloads. The decoded payloads of POST requests in my report necessarily show what TrustedForm's client-side source code intercepts ***before*** any encoding or encryption is employed by TrustedForm's client-side source code and while the user form input data is "in transit" to TrustedForm's server. In other words, ActiveProspect intercepts the user's form inputs in plain language as the user is sending them from their browser, and only after the inputs are intercepted (while they are still in transit) does ActiveProspect apply any encoding or encryption. The intercepted user form input data is then sent to TrustedForm's server contemporaneously as the user fills out Prudential's webform. The plot above in paragraph 54 clearly depicts the contemporaneous nature of interception and collection of user form input data by ActiveProspect.

116. In addition, individual transmissions of 'events' POST requests include sufficient context for their meaning to be plain and comprehensible. For example, not only does TrustedForm capture each keystroke as a separate event, each event payload includes the context of the previous letters typed in the same field. Take requests 53-70 in the

[139] Polish Decl. 117
[140] Polish Decl. 118

Translated Events Payload as an example, shown below. The sequence of events show the letters of an email address being typed into the form. The final event in this form field, request 70, includes not just the final letter, but the entire email address in plain text.

Figure: Timeseries of user form input data intercepted by TrustedForm's source code and sent to TrustedForm's server as a user types in email address on the life insurance form on Prudential's website. The red highlights show that each transmission contains the specific key that was pressed as well as the context of complete value of the form field in the same transmission.

117. It is noteworthy that the entire email address was included in the payload of the POST request 70 in the Translated Events Payload document, which was obtained by simply decoding the POST request sent by TrustedForm's source code to TrustedForm's server during my testing on term.prudential.com.

118. During my inspection [redacted]

119. As another example, requests 33-38 in my testing reflect the content typed into the field for "first name." The final event in that field, request 38, includes not just the letter "r" but then entire entry into the field, "Zubair," as shown below.

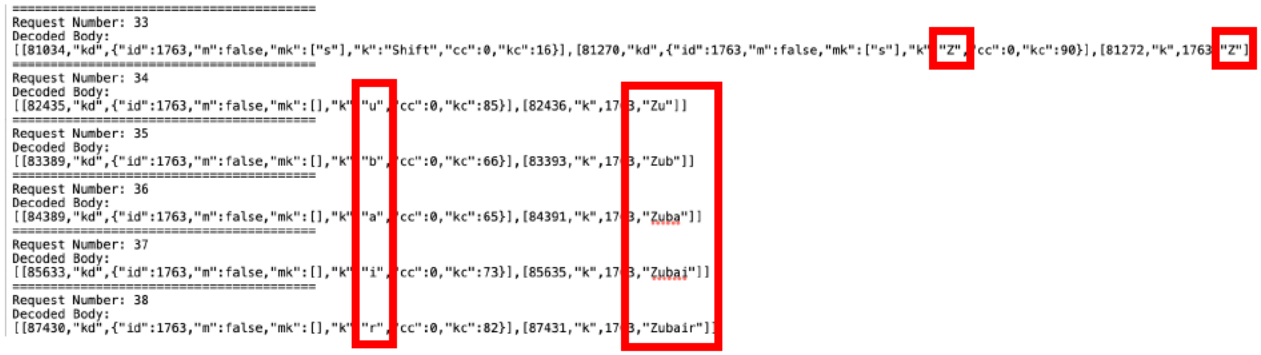


Figure: Timeseries of user form input data intercepted by TrustedForm's source code and sent to TrustedForm's server as a user types in first name on the life insurance form on Prudential's website. The red highlights show that each transmission contains the specific key that was pressed as well as the context of complete value of the form field in the same transmission.

120. As another example, requests 40-45 in my testing reflect the content typed into the field for "last name." The final event in that field, request 45, includes not just the letter "q" but then entire entry into the field, "Shafiq," as shown below.

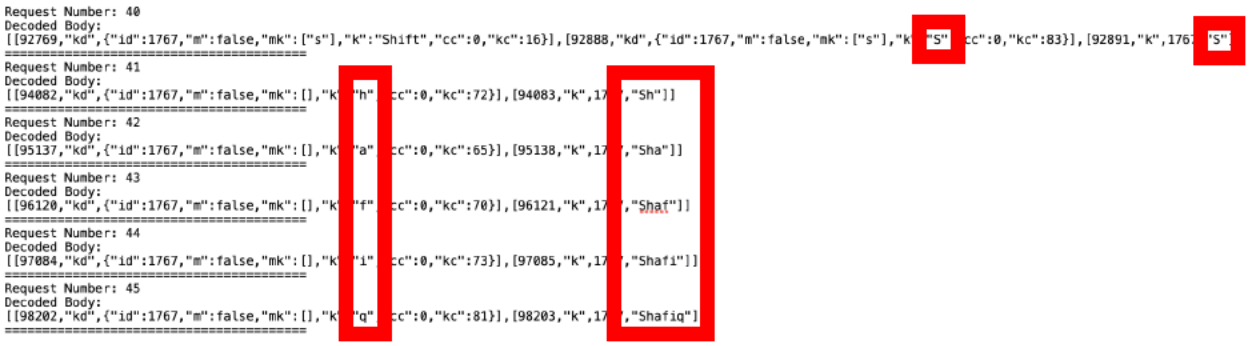


Figure: Timeseries of user form input data intercepted by TrustedForm's source code and sent to TrustedForm's server as a user types in last name on the life insurance form on Prudential's website. The red highlights show that each transmission contains the specific key that was pressed as well as the context of complete value of the form field in the same transmission.

121. Based on the foregoing, I conclude that the interception by TrustedForm's source code is "in transit" and "contemporaneous" as well as TrustedForm's source code expressly reads the content of user form inputs to analyze whether the input data is, for example, an email address or phone number.

VIII. CONCLUSIONS

122. My testing and analysis show that (1) Prudential and Assurance IQ installed ActiveProspect's source code on its website to intercept in real time data that users input into Prudential's webform and sent it to ActiveProspect; (2) data in possession of Prudential, Assurance IQ, and ActiveProspect can be used to identify natural persons whose form input data was intercepted by ActiveProspect when they filled out a webform to request a life insurance quote on Prudential's website during the Class Period; (3) ActiveProspect can use the form input data intercepted by TrustedForm source code on Prudential's webform during the Class Period; (4) ActiveProspect's TrustedForm source code analyzes the substance of the form input data as it intercepts that data from Prudential's webform and while it is in transit during the Class Period.

123. I reserve the right to amend, modify, or supplement my opinions as new or additional information becomes available to me in advance of trial.

DATED:

Zubair Shafiq

APPENDIX A

3043 Kemper Hall
Davis, CA, 95616 USA
zubair@ucdavis.edu
www.cs.ucdavis.edu/~zubair

Zubair Shafiq

Research Interests

Web Privacy, Safety, and Security

Professional Experience

2020– **Associate Professor**
Department of Computer Science, University of California-Davis

2014–2020 **Assistant Professor**
Department of Computer Science, University of Iowa

2009–2014 **Research Assistant**
Department of Computer Science and Engineering, Michigan State University

2013 **Research Intern**
IBM T. J. Watson Research Center

2012 **Research Intern**
Telefonica Research

2011 **Research Intern**
AT&T Labs – Research

2007-2009 **Research Engineer**
Next Generation Intelligent Networks Research Center, Pakistan

Education

2009–2014 **Ph.D. Computer Science**
Department of Computer Science and Engineering, Michigan State University

2004–2008 **B.E. Electrical Engineering**
National University of Sciences & Technology (NUST), Pakistan

Honors and Awards

2024 **Distinguished Artifact Award** ACM Conference on Computer and Communications Security
2024 **Caspar Bowden Award**, Runner-up for Outstanding Research in Privacy Enhancing Technologies
2023 **Best Paper Award**, ACM Internet Measurement Conference
2023 **Chancellor's Fellow**, University of California Davis
2020 **Research Highlights**, Communications of the ACM
2020 **Dean's Scholar Award**, University of Iowa
2018 **NSF Faculty Early Career Development (CAREER) Award**
2018 **Andreas Pfitzmann Award**, Best Student Paper at Privacy Enhancing Technologies Symposium
2017 **Best Paper Award**, ACM Internet Measurement Conference
2015 **NSF CISE Research Initiation Initiative (CRII) Award**
2013 **Fitch-Beach Outstanding Graduate Research Award**, Michigan State University

2012 **Best Paper Award**, IEEE International Conference on Network Protocols

2007, 2008 **Dean's Plaque of Excellence**, National University of Sciences & Technology, Pakistan

Publications

SM+S **Auditing the Compliance and Enforcement of Twitter's Advertising Policies**
Yash Vekaria, Zubair Shafiq, Savvas Zannettou
Social Media and Society Journal, 2025

ICWSM **Towards Characterizing and Detecting Incentivized Reviews on eCommerce Platforms**
Rajvardhan Oak, Zubair Shafiq
AAAI International Conference on Web and Social Media, 2025

TOPS **AutoFR: Automated Filter Rule Generation for Adblocking**
Hieu Le, Salma Elmalaki, Athina Markopoulou, Zubair Shafiq
ACM Transactions on Privacy and Security, 2024

IMC **Watching TV with the Second-Party: A First Look at Automatic Content Recognition Tracking in Smart TVs**
Gianluca Anselmi, Yash Vekaria, Alexander D'Souza, Patricia Callejo, Anna Maria Mandalari, Zubair Shafiq
ACM Internet Measurement Conference, 2024

CCS **Blocking Tracking JavaScript at the Function Granularity**
Abdul Haddi Amjad, Shaoor Munir, Zubair Shafiq, Muhammad Ali Gulzar
ACM Conference on Computer and Communications Security, 2024

USENIX Security **PURL: Safe and Effective Sanitization of Link Decoration**
Shaoor Munir, Patrick Lee, Umar Iqbal, Zubair Shafiq, Sandra Siby
USENIX Security Symposium, 2024

JETLaw **Google's Chrome Antitrust Paradox**
Shaoor Munir, Konrad Kollnig, Anastasia Shuba, Zubair Shafiq
Vanderbilt Journal of Entertainment and Technology Law, 2024

IMWUT/ UbiComp **Aragorn: A Privacy-Enhancing System for Mobile Cameras**
Hari Venugopalan, Zainul Abi Din, Trevor Carpenter, Jason Lowe-Power, Sam King, Zubair Shafiq
ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2024

CHI **Understanding Underground Incentivized Review Services**
Rajvardhan Oak, Zubair Shafiq
ACM Conference on Human Factors in Computing Systems, 2024

S&P **The Inventory is Dark and Full of Misinformation: Understanding the Abuse of Ad Inventory Pooling in the Ad-Tech Supply Chain**
Yash Vekaria, Rishab Nithyanand, Zubair Shafiq
IEEE Symposium on Security & Privacy, 2024

CSR **Harnessing TI Feeds for Exploitation Detection**
Kajal Patel, Zubair Shafiq, Mateus Nogueira, Daniel Sadoc Menasché, Enrico Lovat, Taimur Kashif, Ashton Woiwood, Matheus Martins
IEEE International Conference on Cyber Security and Resilience, 2024

JOLT **A Scientific Approach to Tech Accountability**
Woodrow Hartzog, Scott Jordan, David Choffnes, Athina Markopoulou, Zubair Shafiq
Beyond the FTC: The Future of Privacy Enforcement, Harvard Journal of Law & Technology, 2023

PNAS **Auditing YouTube's Recommendation System for Ideologically Congenial, Extreme, and Problematic Recommendations**
Muhammad Haroon, Magdalena Wojcieszak, Anshuman Chhabra, Xin Liu, Prasant Mohapatra, Zubair Shafiq
Proceedings of the National Academy of Sciences (PNAS), 2023

IMC **Tracking, Profiling, and Ad Targeting in the Alexa Echo Smart Speaker Ecosystem**
Umar Iqbal, Pouneh Nikkhah Bahrami, Rahmadi Trimananda, Hao Cui, Alexander Gamero-Garrido, Daniel Dubois, David Choffnes, Athina Markopoulou, Franziska Roesner, Zubair Shafiq
ACM Internet Measurement Conference, 2023
Best Paper Award

PETS **A Utility-Preserving Obfuscation Approach for YouTube Recommendations**
Jiang Zhang, Hadi Askari, Konstantinos Psounis, Zubair Shafiq
Privacy Enhancing Technologies Symposium, 2023

PETS **Blocking JavaScript without Breaking the Web**
Abdul Haddi Amjad, Zubair Shafiq, Muhammad Ali Gulzar
Privacy Enhancing Technologies Symposium, 2023

CCS **CookieGraph: Measuring and Countering First-Party Tracking Cookies**
Shaoor Munir, Sandra Siby, Umar Iqbal, Steven Englehardt, Zubair Shafiq, Carmela Troncoso
ACM Conference on Computer and Communications Security, 2023

S&P **Accuracy-Privacy Trade-off in Deep Ensemble: A Membership Inference Perspective**
Shahbaz Rezaei, Zubair Shafiq, Xin Liu
IEEE Symposium on Security & Privacy, 2023

USENIX Security **AutoFR: Automated Filter Rule Generation for Adblocking**
Hieu Le, Salma Elmalaki, Athina Markopoulou, Zubair Shafiq
USENIX Security Symposium, 2023

NDSS **Harpo: Learning to Subvert Online Behavioral Advertising**
Jiang Zhang, Konstantinos Psounis, Muhammad Haroon, Zubair Shafiq
Network and Distributed System Security Symposium, 2022

USENIX Security **WebGraph: Capturing Advertising and Tracking Information Flows for Robust Blocking**
Sandra Siby, Umar Iqbal, Steven Englehardt, Zubair Shafiq, Carmela Troncoso
USENIX Security Symposium, 2022

USENIX Security **Khaleesi: Breaker of Advertising and Tracking Request Chains**
Umar Iqbal, Charlie Wolfe, Charles Nguyen, Steven Englehardt, Zubair Shafiq
USENIX Security Symposium, 2022

PETS **FP-Radar: Longitudinal Measurement and Early Detection of Browser Fingerprinting**
Pouneh Nikkhah Bahrami, Umar Iqbal, Zubair Shafiq
Privacy Enhancing Technologies Symposium, 2022

ACL **Adversarial Authorship Attribution for Deobfuscation**
Wanyue Zhai, Jonathan Rusert, Zubair Shafiq, Padmini Srinivasan
Association for Computational Linguistics, 2022

ACL **On the Robustness of Offensive Language Classifiers**
Jonathan Rusert, Zubair Shafiq, Padmini Srinivasan
Association for Computational Linguistics, 2022

EuroS&P **DNN Model Architecture Fingerprinting Attack on CPU-GPU Edge Devices**
Kartik Patwari, Syed Mahbub Hafiz, Han Wang, Houman Homayoun, Zubair Shafiq, Chen-Nee Chuah
IEEE European Symposium on Security and Privacy, 2022

DATE **Stealthy Inference Attack on DNN via Cache-based Side-channel Attacks**
Han Wang, Syed Mahbub Hafiz, Kartik Patwari, Chen-Nee Chuah, Zubair Shafiq, Houman Homayoun
IEEE/ACM Design Automation and Test in Europe, 2022

IMC **TrackerSift: Untangling Mixed Tracking and Functional Web Resources**
Abdul Haddi Amjad, Danial Saleem, Fareed Zaffar, Muhammad Ali Gulzar, Zubair Shafiq
ACM Internet Measurement Conference, 2021

S&P **Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors**
Umar Iqbal, Steven Englehardt, Zubair Shafiq
IEEE Symposium on Security & Privacy, 2021

NDSS **CV-Inspector: Towards Automating Detection of Adblock Circumvention**
Hieu Le, Athina Markopoulou, Zubair Shafiq
Network and Distributed System Security Symposium, 2021

EACL **Through the Looking Glass: Learning to Attribute Synthetic Text Generated by Language Models**
Shaoor Munirl, Brishna Batool, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
European Chapter of the Association for Computational Linguistics, 2021

IMC **Understanding Incentivized Mobile App Installs on Google Play Store**
Shehroze Farooqi, Alvaro Feal, Tobias Lauinger, Damon McCoy, Zubair Shafiq, Narseo Vallina-Rodriguez
ACM Internet Measurement Conference, 2020

ACL **A Girl Has A Name: Detecting Authorship Obfuscation**
Asad Mahmood, Zubair Shafiq, Padmini Srinivasan
Annual Conference of the Association for Computational Linguistics, 2020

S&P **AdGraph: A Graph-Based Approach to Ad and Tracker Blocking**
Umar Iqbal, Peter Snyder, Shitong Zhu, Benjamin Livshits, Zhiyun Qian, Zubair Shafiq
IEEE Symposium on Security & Privacy, San Francisco, 2020

PETS **CanaryTrap: Detecting Data Misuse by Third-Party Apps on Online Social Networks**
Shehroze Farooqi, Maaz Musa, Zubair Shafiq, Fareed Zaffar
Privacy Enhancing Technologies Symposium, Montreal, 2020

PETS **Inferring Tracker-Advertiser Relationships in the Online Advertising Ecosystem**
John Cook, Rishab Nithyanand, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Montreal, 2020

PETS **The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking**
Janus Varmarken, Hieu Le, Anastasia Shuba, Zubair Shafiq, Athina Markopoulou
Privacy Enhancing Technologies Symposium, Montreal, 2020

IoTDI **Characterizing Smart Home IoT Traffic in the Wild**
M. Hammad Mazhar, Zubair Shafiq
ACM/IEEE Conference on Internet of Things Design and Implementation, Sydney, 2020

PAM **FlowTrace: A Framework for Active Bandwidth Measurements using In-band Packet Trains**
Adnan Ahmed, Ricky Mok, Zubair Shafiq
Passive and Active Measurement Conference, Eugene, 2020

PETS **A Girl Has No Name: Automated Authorship Obfuscation using X-Mutant**
Asad Mahmood, Faizan Ahmad, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
Privacy Enhancing Technologies Symposium, Stockholm, 2019

PETS **No Place to Hide: Inadvertent Location Privacy Leaks on Twitter**
Jonathan Rusert, Osama Khalid, Dat Hong, Zubair Shafiq, Padmini Srinivasan
Privacy Enhancing Technologies Symposium, Stockholm, 2019

WWW **Measurement and Early Detection of Third-Party Application Abuse on Twitter**
Shehroze Farooqi, Zubair Shafiq
The Web Conference (WWW), San Francisco, 2019

WWW **ShadowBlock: A Lightweight and Stealthy Adblocking Browser**
Shitong Zhu, Umar Iqbal, Zhongjie Wang, Zhiyun Qian, Zubair Shafiq, Weiteng Chen
The Web Conference (WWW), San Francisco, 2019

WWW **Measuring Political Personalization of Google News Search**
Huyen Le, Raven Maragh, Brian Ekdale, Timothy Havens, Andrew High, Zubair Shafiq
The Web Conference (WWW), San Francisco, 2019

ASONAM **A Postmortem of Suspended Twitter Accounts in the 2016 U.S. Presidential Election**
Huyen Le, Bob Boynton, Zubair Shafiq, Padmini Srinivasan
IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Vancouver, 2019

TDSC **Large Scale Characterization of Software Vulnerability Life Cycles**
Muhammad Shahzad, Zubair Shafiq, Alex X. Liu
IEEE Transactions on Dependable and Secure Computing, 2019

PETS **NoMoAds: Effective and Efficient Cross-App Mobile Ad-Blocking**
Anastasia Shuba, Athina Markopoulou, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Barcelona, 2018
Andreas Pfitzmann Best Student Paper Award

NDSS **Measuring and Disrupting Anti-Adblockers Using Differential Execution Analysis**
Shitong Zhu, Xunchao Hu, Zhiyun Qian, Zubair Shafiq, Heng Yin
Network and Distributed System Security Symposium, San Diego, 2018

INFOCOM **Real-time Video Quality of Experience Monitoring for HTTPS and QUIC**
M. Hammad Mazhar, Zubair Shafiq
IEEE International Conference on Computer Communications, Honolulu, 2018

TON **Optimizing Internet Transit Routing for Content Delivery Networks**
Faraz Ahmed, Zubair Shafiq, Amir Khakpour, Alex Liu
IEEE/ACM Transactions on Networking, 2018

TBD **Optimizing Taxi Driver Profit Efficiency: A Spatial Network-based Markov Decision Process Approach**
Xun Zhou, Huigui Rong, Chang Yang, Qun Zhang, Amin Vahedian Khezerlou, Hui Zheng, Zubair Shafiq, Alex Liu
IEEE Transactions on Big Data, 2018

TOPS **Measuring, Characterizing, and Detecting Facebook Like Farms**
Muhammad Ikram, Lucky Onwuzurike, Shehroze Farooqi, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq
ACM Transactions on Privacy and Security, 2017

TIST **A Traffic Flow Approach to Early Detection of Gathering Events: Comprehensive Results**
Amin Khezerlou, Xun Zhou, Lufan Li, Zubair Shafiq, Alex X. Liu, Fan Zhang
ACM Transactions on Intelligent Systems and Technology, 2017

IMC **Measuring and Mitigating OAuth Access Token Abuse by Collusion Networks**
Shehroze Farooqi, Fareed Zaffar, Nektarios Leontiadis, Zubair Shafiq
ACM Internet Measurement Conference, London, 2017
Best Paper Award
CACM Research Highlights 2020

IMC **The Ad Wars: Retrospective Measurement and Analysis of Anti-Adblock Filter Lists**
Umar Iqbal, Zubair Shafiq, Zhiyun Qian
ACM Internet Measurement Conference, London, 2017

SIGMETRICS **Characterizing and Modeling Patching Practices of Industrial Control Systems**
Brandon Wang, Xiaoye Li, Leandro P. de Aguiar, Daniel S. Menasche, Zubair Shafiq
ACM International Conference on Measurement and Modeling of Computer Systems, Urbana-Champaign, 2017

PETS **Detecting Anti Ad-blockers in the Wild**
Muhammad Haris Mughees, Zhiyun Qian, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Minneapolis, 2017

ICDM **Accurate Detection of Automatically Spun Content via Stylometric Analysis**
Usman Shahid, Shehroze Farooqi, Raza Ahmad, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
IEEE International Conference on Data Mining, New Orleans, 2017

CHI **Revisiting The American Voter on Twitter**
Huyen Le, G.R. Boynton, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan
ACM Conference on Human Factors in Computing Systems, Denver, 2017

ICDCS **Distributed Load Balancing in Key-Value Networked Caches**
Sikder Huq, Zubair Shafiq, Sukumar Ghosh, Amir Khakpour, Harkeerat Bedi
IEEE International Conference on Distributed Computing Systems, Atlanta, 2017

ICNP **Peering vs. Transit: Performance Comparison of Peering and Transit Interconnections**
Adnan Ahmed, Zubair Shafiq, Harkeerat Bedi, Amir Khakpour
IEEE International Conference on Network Protocols, Toronto, 2017

ICNP **Suffering from Buffering? Detecting QoE Impairments in Live Video Streams**
Adnan Ahmed, Zubair Shafiq, Harkeerat Bedi, Amir Khakpour
IEEE International Conference on Network Protocols, Toronto, 2017

ICNP **Multipath TCP Traffic Diversion Attacks and Countermeasures**
Ali Munir, Zhiyun Qian, Zubair Shafiq, Alex Liu, Franck Le
IEEE International Conference on Network Protocols, Toronto, 2017

ICWSM **Scalable News Slant Measurement Using Twitter**
Huyen Le, Zubair Shafiq, Padmini Srinivasan
AAAI International Conference on Web and Social Media, 2017

HT **Bumps and Bruises: Mining Presidential Campaign Announcements on Twitter**
Huyen Le, G.R. Boynton, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan
ACM Conference on Hypertext and Social Media, Prague, 2017

Networking **Cascade Size Prediction in Online Social Networks**
Zubair Shafiq, Alex Liu
IFIP Networking, Prague, 2017
Best Paper Award Candidate (3 nominations out of 43 accepted papers)

Networking **A Graph Theoretic Approach to Fast and Accurate Malware Detection**
Zubair Shafiq, Alex Liu
IFIP Networking, Prague, 2017

eCrime **Characterizing Key Stakeholders in an Online Black-Hat Marketplace**
Shehroze Farooqi, Muhammad Ikram, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq, Fareed Zaffar
IEEE/APWG Symposium on Electronic Crime Research, Prague, 2017

ICNP **Optimizing Internet Transit Routing for Content Delivery Networks**
Faraz Ahmed, Zubair Shafiq, Amir Khakpour, Alex Liu
IEEE International Conference on Network Protocols, Singapore, 2016

DSN **Malware Slums: Measurement and Analysis of Malware on Traffic Exchanges**
Salman Yousaf, Umar Iqbal, Shehroze Farooqi, Raza Ahmad, Zubair Shafiq, Fareed Zaffar
IEEE/IFIP International Conference on Dependable Systems and Networks, France, 2016

SIGMETRICS **QoE Analysis of a Large-Scale Live Video Streaming Event**
Adnan Ahmed, Zubair Shafiq, Amir R. Khakpour
ACM International Conference on Measurement and Modeling of Computer Systems, France, 2016

ICDCS **The Internet is For Porn: Measurement and Analysis of Online Adult Traffic**
Faraz Ahmed, Zubair Shafiq, Alex X. Liu
IEEE International Conference on Distributed Computing Systems, Japan, 2016

INFOCOM **Characterizing Caching Workload of a Large Commercial Content Delivery Network**
Zubair Shafiq, Amir R. Khakpour, Alex X. Liu
IEEE International Conference on Computer Communications, San Francisco, 2016

SIGSPATIAL **A Traffic Flow Approach to Early Detection of Gathering Events**
Xun Zhou, Amin Vahedian Khezerlou, Alex Liu, Zubair Shafiq, Fan Zhang
ACM International Conference on Advances in Geographic Information Systems, San Francisco, 2016

CIKM **The Rich and the Poor: A Markov Decision Process Approach to Optimizing Taxi Driver Revenue Efficiency**
Huigui Rong, Xun Zhou, Chang Yang, Zubair Shafiq, Alex Liu
ACM International Conference on Information and Knowledge Management, Indianapolis, 2016

TON **Characterizing and Optimizing Cellular Network Performance during Crowded Events**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Shobha Venkataraman, Jia Wang
IEEE/ACM Transactions on Networking, 2016

SMP **What Campaigns Become as Social Media Become the Infrastructure of Political Communication**
G.R. Boynton, Huyen Le, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan
Social Media and Politics, 2016

TMC **Geospatial and Temporal Dynamics of Application Usage in Cellular Data Networks**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
IEEE Transactions on Mobile Computing, 2015

NSF/FCC QoE **Tracking Mobile Video QoE in the Encrypted Internet**
Zubair Shafiq
NSF/FCC Workshop on Tracking Quality of Experience in the Internet, Princeton, 2015

NSF/FCC QoE **Bidirectional Crosslayer QoE Optimization**
Srikanth Sundaresan, Zubair Shafiq
NSF/FCC Workshop on Tracking Quality of Experience in the Internet, Princeton, 2015

IMC **Paying for Likes? Understanding Facebook Like Fraud Using Honeypots**
Emiliano De Cristofaro, Arik Friedmam, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq
ACM Internet Measurement Conference, 2014

SIGMETRICS **Understanding the Impact of Network Dynamics on Mobile Video User Engagement**
Zubair Shafiq, Jeffrey Erman, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
ACM International Conference on Measurement and Modeling of Computer Systems, 2014

SIGMETRICS **Revisiting Caching in Content Delivery Networks**
Zubair Shafiq, Alex X. Liu, Amir Khakpour
ACM International Conference on Measurement and Modeling of Computer Systems, 2014

SIGMETRICS **A First Look at Cellular Network Performance during Crowded Events**
Zubair Shafiq, Alex X. Liu, Amir Khakpour
ACM International Conference on Measurement and Modeling of Computer Systems, 2013

ICNP **Who are You Talking to? Breaching Privacy in Encrypted IM Networks**
Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha
IEEE International Conference on Network Protocols, 2013

CSCW **Is News Sharing on Twitter Ideologically Biased?**
Jonathan Morgan, Cliff Lampe, Zubair Shafiq
ACM Conference on Computer Supported Cooperative Work and Social Computing, 2013

ACM HotNets **Cross-Path Inference Attacks on Multipath TCP**
Zubair Shafiq, Franck Le, Mudhakar Srivatsa, Alex X. Liu
ACM Workshop on Hot Topics in Networks, 2013

TON **Large Scale Measurement and Characterization of Cellular Machine-to-Machine Traffic**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
IEEE/ACM Transactions on Networking, 2013

JSAC **Identifying Leaders and Followers in Online Social Networks**
Zubair Shafiq, Muhammad U. Ilyas, Alex X. Liu, Hayder Radha
IEEE Journal on Selected Areas in Communications, 2013

JSAC **A Distributed Algorithm for Identifying Information Hubs in Social Networks**
Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha
IEEE Journal on Selected Areas in Communications, 2013

JNSM **TCAMChecker: A Software Approach to the Error Detection and Correction of TCAM-based Networking Systems**
Zubair Shafiq, Chad Meiners, Alex Liu, Ke Shen, Zheng Qin
Springer Journal of Network and Systems Management, 2012

ICNP **A Semantics Aware Approach to Automated Reverse Engineering Unknown Protocols**
Yipeng Wang, Xiaochun Yun, Zubair Shafiq, Alex X. Liu, Zhibin Zhang, Liyan Wang, Danfeng (Daphne) Yao, Yongzheng Zhang, Li Guo
IEEE International Conference on Network Protocols, 2012
Best Paper Award

SIGMETRICS **A First Look at Cellular Machine-to-Machine Traffic – Large Scale Measurement and Characterization**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
ACM International Conference on Measurement and Modeling of Computer Systems, London, 2012

ICSE **A Large Scale Exploratory Analysis of Software Vulnerability Life Cycles**
Muhammad Shahzad, Zubair Shafiq, Alex X. Liu
International Conference on Software Engineering, Switzerland, 2012

INFOCOM **Characterizing Geospatial Dynamics of Application Usage in a 3G Cellular Data Network**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
IEEE Conference on Computer Communications, Orlando, 2012

SIGMETRICS **Characterizing and Modeling Internet Traffic Dynamics of Cellular Devices**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jia Wang
ACM International Conference on Measurement and Modeling of Computer Systems, San Jose, 2011

Networking **A Random Walk Approach to Modeling the Dynamics of the Blogosphere**
Zubair Shafiq, Alex X. Liu
IFIP Networking, Spain, 2011

INFOCOM **A Distributed and Privacy-Preserving Algorithm for Identifying Information Hubs in Social Networks**
Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha
IEEE Conference on Computer Communications, Spain, 2011

RAID **PE-Miner: Mining Structural Information to Detect Malicious Executables in Realtime**
Zubair Shafiq, Syeda Momina Tabish, Fauzan Mirza, Muddassar Farooq
International Symposium On Recent Advances In Intrusion Detection, France, 2009

GECCO **Evolvable Malware**
Sadia Noreen, Shafaq Murtaza, Zubair Shafiq, Muddassar Farooq
ACM Genetic and Evolutionary Computation Conference, Canada, 2009

CCS AISec **Using Spatio-Temporal Information in API Calls with Machine Learning Algorithms for Malware Detection and Analysis**
Faraz Ahmed, Haider Hameed, Zubair Shafiq, Muddassar Farooq
Workshop on Security and Artificial Intelligence, ACM Conference on Computer & Communications Security, Chicago, 2009

KDD CSI **Malware Detection using Statistical Analysis of Byte-Level File Content**
Syeda Momina Tabish, Zubair Shafiq, Muddassar Farooq
Workshop on CyberSecurity and Intelligence Informatics (CSI), ACM Conference on Knowledge Discovery and Data Mining, France, 2009

VB **PE-Probe: leveraging packer detection and structural information to detect malicious portable executables**
Zubair Shafiq, Syeda Momina Tabish, Muddassar Farooq
Virus Bulletin, Switzerland, 2009

DIMVA **Embedded Malware Detection using Markov n-grams**
Zubair Shafiq, Syed Ali Khayam, Muddassar Farooq
International Conference on Detection of Intrusions, Malware and Vulnerability Assessment, France, 2008

GECCO **Improving Accuracy of Immune Inspired Malware Detectors using Intelligent Features**
Zubair Shafiq, Syed Ali Khayam, Muddassar Farooq
ACM Genetic and Evolutionary Computation Conference, Atlanta, 2008

Funding

External Competitive Research Grants

NSF-SaTC-EAGER **News and Public Affairs Information**
National Science Foundation
PI, Duration: 2024-2026, Total: $300,000, Personnel: Magdalena Wojcieszak (PI), Zubair Shafiq (Co-PI)

UC **Auditing Compliance of Data Privacy Laws in California**
UC Partnerships in Computational Transformation
PI, Duration: 2022-2023, Total: $160,000, Share: $80,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine); Gene Tsudik (Co-PI: UC Irvine)

NSF-SaTC **Defending against Emerging Stateless Web Tracking**
National Science Foundation
PI, Duration: 2022-2026, Total: $1,200,000, Share: $400,000
Personnel: Zubair Shafiq (PI: UC Davis); Alexandros Kapravelos (PI: NC State); Anupam Das (Co-PI: NC State)

CITRIS and the Banatao Institute **Auditing the compliance of California consumer privacy regulations at scale**
Center for Information Technology Research in the Interest of Society (CITRIS)
Co-PI, Duration: 2021-2022, Total: $60,000, Share: $20,000
Personnel: Serge Egelman (Co-PI: UC Berkeley); Zubair Shafiq (Co-PI: UC Davis)

NSF-SaTC-Frontier **Protecting Personal Data Flow on the Internet**
National Science Foundation
PI, Duration: 2020-2025, Total: $10,000,000, Share: $1,100,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine); Konstantinos Psounis (PI: USC); David Choffnes (PI: Northeastern)

NSF-CAREER **Quality of Experience and Network Management in the Encrypted Internet**
National Science Foundation
PI, Duration: 2018-2023, Total: $500,000, Share: $500,000
Personnel: Zubair Shafiq (PI: UC Davis)

NSF-SaTC **A Multi-Layer Learning Approach to Mobile Traffic Filtering**
National Science Foundation
PI, Duration: 2018-2021, Total: $500,000, Share: $250,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine)

NSF-SaTC **The Web Ad Technology Arms Race: Measurement, Analysis, and Countermeasures**
National Science Foundation
PI, Duration: 2017-2020, Total: $500,000 + $16,000 (REU Supplement 2019) + $16,000 (REU Supplement 2021), Share: $282,000
Personnel: Zubair Shafiq (PI: UC Davis); Zhiyun Qian (PI: UC Riverside)

NSF-NeTS **Towards Scalable and Energy Efficient Cellular IoT Communication**
National Science Foundation
PI, Duration: 2016-2019, Total: $500,000, Share: $166,000
Personnel: Zubair Shafiq (PI: Iowa); K.K. Ramakrishnan (PI: UC Riverside); Koushik Kar (PI: RPI)

NSF-SaTC **Multipath TCP Side Channel Vulnerabilities and Defenses**
National Science Foundation
PI, Duration: 2015-2018, Total: $500,000, Share: $167,000
Personnel: Zubair Shafiq (PI: Iowa); Zhiyun Qian (PI: UC Riverside); Alex Liu (PI: Michigan State University)

NSF-NeTS **Towards Measurement and Optimization of Internet Video Quality of Experience**
National Science Foundation
PI, Duration: 2015-2018, Total: $175,000 + $16,000 (REU Supplement 2016), Share: $191,000
Personnel: Zubair Shafiq (PI: Iowa)

DTL **Detection and Circumvention of Ad-Block Detectors**
Data Transparency Lab
PI, Duration: 2016-2017, Total: $56,000, Share: $28,000
Personnel: Zubair Shafiq (PI: Iowa); Zhiyun Qian (PI: UC Riverside)

Internal Competitive Research Grants

Academic Senate **Socio-Computational Interventions to Mitigate Misinformation in Recommendations**
Noyce Foundation
PI, Duration: 2022-2023, Total: $25,000
Personnel: Magdalena Wojcieszak (PI), Zubair Shafiq (Co-PI)

Noyce **Measuring and Mitigating Biases in Social Recommendation Algorithms**
Noyce Foundation
PI, Duration: 2022-2023, Total: $236,000
Personnel: Zubair Shafiq (PI), Magdalena Wojcieszak (Co-PI)

Noyce **Cross-Layer Approach to Enhance Security/Privacy of AI-enabled IoT Eco-Systems**
Noyce Foundation
Co-PI, Duration: 2022-2023, Total: $225,000
Personnel: Chen-Nee Chuah (PI), Zubair Shafiq (Co-PI), Houman Homayoun (Co-PI)

Noyce **Measuring and Mitigating Biases in Social Recommendation Algorithms**
Noyce Foundation
PI, Duration: 2021-2022, Total: $235,690
Personnel: Zubair Shafiq (PI), Xin Liu (Co-PI), Magdalena Wojcieszak (Co-PI)

Noyce **Cross-Layer Approach to Enhance Security/Privacy of AI-enabled IoT Eco-Systems**
Noyce Foundation
Co-PI, Duration: 2021-2022, Total: $225,000
Personnel: Chen-Nee Chuah (PI), Zubair Shafiq (Co-PI), Houman Homayoun (Co-PI)

UIRF **Social Media Powered Real-Time Digital News Recommendation**
University of Iowa Research Foundation
PI, Duration: 2015-2016, Total: $75,000
Personnel: Zubair Shafiq (PI)

Obermann **Heterogeneous Network Data Analytics to Improve Urban Sustainability**
Obermann Center Interdisciplinary Research Grant
PI, Duration: 2015-2016, Total: $12,000
Personnel: Xun Zhou (PI); Zubair Shafiq (Co-PI)

Industry Grants and Unrestricted Gifts

Siemens PI, Duration: 2021, Total: $60,000, Share: $60,000
Personnel: Zubair Shafiq (PI: UC Davis)

Siemens PI, Duration: 2019, Total: $30,000, Share: $30,000
Personnel: Zubair Shafiq (PI: Iowa)

Siemens PI, Duration: 2018, Total: $60,000, Share: $60,000
Personnel: Zubair Shafiq (PI: Iowa)

Verizon PI, Duration: 2018, Total: $20,000, Share: $20,000
Personnel: Zubair Shafiq (PI: Iowa)

Minim PI, Duration: 2018, Total: $66,164, Share: $66,164
Personnel: Zubair Shafiq (PI: Iowa)

Siemens PI, Duration: 2017, Total: $30,000, Share: $30,000
Personnel: Zubair Shafiq (PI: Iowa)

Nokia PI, Duration: 2017, Total: $53,200, Share: $53,200
Personnel: Zubair Shafiq (PI: Iowa)

Futurewei PI, Duration: 2017, Total: $100,384, Share: $100,384
Personnel: Zubair Shafiq (PI: Iowa)

Facebook PI, Duration: 2016, Total: $8,400, Share: $8,400
Personnel: Zubair Shafiq (PI: Iowa)

Teaching

ECS 152A **Computer Networks**
Fall 2024, University of California at Davis

ECS 289M **Topics in Privacy**
Spring 2024, University of California at Davis

ECS 188 **Ethics in an Age of Technology**
Winter 2024, University of California at Davis

ECS 152A **Computer Networks**
Fall 2023, University of California at Davis

FYS **Big Data, Big Brother**
Winter 2023, University of California at Davis

ECS 289M **Network Security & Privacy**
Winter 2023, University of California at Davis

ECS 152A **Computer Networks**
Fall 2022, University of California at Davis

ECS 152A **Computer Networks**
Spring 2022, University of California at Davis

ECS 153 **Computer Security**
Winter 2022, University of California at Davis

ECS 289M **Data-Driven Security**
Spring 2021, University of California at Davis

ECS 152B **Computer Networks**
Winter 2021, University of California at Davis

CS 2620 **Networking & Security for Informatics**
Spring 2020, The University of Iowa

CS 4980 **Online Advertising & Tracking**
Fall 2019, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2019, The University of Iowa

CS 4980 **Internet Measurement**
Fall 2018, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2018, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2017, The University of Iowa

CS 4980 **Network Security and Privacy**
Fall 2016, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2016, The University of Iowa

CS 4980 **Advanced Computer Networks**
Fall 2015, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2015, The University of Iowa

CS 4980 **Internet Measurement**
Fall 2014, The University of Iowa

Students

Doctorate

2024-current Muhammad Jazlan

2022-current Rajvardhan Oak

2021-current Pouneh Nikkhah Bahrami

2021-current Shaoor Munir

2021-current Yash Vekaria

2021-current Hari Venugopalan (co-advised with Sam King)

2016-2021 Dr. Umar Iqbal; First Position: CIFellow/Postdoc, University of Washington

2015-2021 Dr. Shehroze Farooqi; First Position: Researcher, Palo Alto Networks

2015-2019 Dr. Huyen Le; First Position: Postdoc, National Center for Toxicological Research

Select Recent Masters Mentees

2021 Mohammad Ismail Daud
2021 Sunshine Chong
2021 Rachit Dhamija
2020 Pouneh Nikkhah Bahrami
2018 Daniel Zhou
2016-2017 Sai Kalyan Moguloju

Select Recent Undergraduate Mentees

2024 Jonathan Levitsky
2023 Divya Raj
2023 Shuaib Ahmed
2023 Ryan Swift
2023 Tangbaihe (Mona) Wang
2023 Patrick Lee
2022 Jake Smith
2022 Christina Phan
2022 Kev Rockwell
2020-2022 Kajal Patel (NSF REU)
2020-2022 Wanyue Zhai (graduate student at Stanford)
2020-2022 Ray Ngan (NSF REU) (industry: Palo Alto Networks)
2020-2021 Surya Konkimalla
2020-2021 Charles Nguyen (industry: Apple)
2019-2021 Charlie Wolfe (NSF REU) (industry: Apple)
2021 Caelan MacArthur (NSF DREU)
2020-2021 Taimur Kashif (NSF REU) (industry: VMWare)
2019-2020 Ashton Woiwood (NSF REU)
2018 Basil Chatha
2017 Treyton Krupp (NSF REU)
2017 Daniel Zhou (NSF REU)
2017 Gabriel Akanni (SROP)
2016-2017 Xiaoye Li (NSF REU)
2016 Yu Dai

High School

2023 Reeva Rao
2023 Jayalakshmi Raffill
2019 Kathy Zhong
2018 Alice Martynova
2017 William Kim
2016 Brandon Wang

External Service

PC Co-Chair Privacy Enhancing Technologies Symposium (PETs), 2025

PC Co-Chair	Privacy Enhancing Technologies Symposium (PETs), 2024
PC Co-Chair	Workshop on Technology and Consumer Protection (ConPro'23), IEEE Symposium on Security & Privacy ("Oakland")
PC Co-Chair	Workshop on Technology and Consumer Protection (ConPro'22), IEEE Symposium on Security & Privacy ("Oakland")
PC Co-Chair	Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb'23), Network and Distributed System Security Symposium (NDSS)
PC Co-Chair	Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb'22), Network and Distributed System Security Symposium (NDSS)
Publicity Co-Chair	ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2020)
Co-Chair	NSF NeTS Early Career Investigators Workshop 2019
PC Co-Chair	Student Workshop - ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2018)
PC Co-Chair	WWW 8th International Workshop on Location and the Web (LocWeb 2018)
Poster Chair	ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2018)
Technical Committee	Elsevier Computer Communications (2015-2019)
Guest Editor	Special Issue on Mobile Traffic Analytics, Elsevier Computer Communications (2016)
Editorial Board	Proceedings on Privacy Enhancing Technologies (PoPETs) (2019, 2020, 2021)
Panelist	NSF (2017, 2018, 2019, 2020, 2021, 2022, 2023)
Conference TPC/Reviewer	IEEE S&P (2022), PETS (2021, 2020, 2019, 2018, 2017), ACM IMC (2021, 2020), ACM CoNEXT (2019), ACM SIGMETRICS (2023, 2022, 2020, 2013), WWW (2020, 2018), ACM CSCW (2018, 2019), IEEE/IFIP TMA (2020, 2019), NDSS MADWeb Workshop (2019), IEEE INFOCOM (2017, 2015, 2010, 2009), ACM WPES (2018), IEEE S&P Consumer Protection Workshop (2021, 2020), ACM SIGCOMM Internet-QoE Workshop (2017), ACM SIGCOMM Workshop on IoT Security and Privacy (2018), WWW CyberSafety Workshop (2018), WWW Workshop on Location and the Web (2018), IEEE ICNP (2014, 2013), MASCOTS (2013), ICDCN (2017, 2018)
Journal Reviewer	IEEE/ACM Transactions on Networking, ACM Transactions on the Web, IEEE Transactions on Mobile Computing, IEEE Transactions on Network and Service Management, ACM Transactions on Multimedia Computing, IEEE Transactions on Cognitive Communications and Networking, ACM SIGCOMM Computer Communication Review, Elsevier Computer Communications, Elsevier Performance Evaluation, Springer Wireless Networks

Internal Service

Chair	Departmental Colloquium Series Department of Computer Science, University of California Davis, 2021-2025
Member	Departmental Awards Committee Department of Computer Science, University of California Davis, 2023-2024
Member	Diversity, Equity, Inclusion Committee College of Engineering, University of California Davis, 2021-2022

Committee	Departmental Graduate Committee Department of Computer Science, University of Iowa, 2019-2020
Chair	Departmental Colloquium Series Department of Computer Science, University of Iowa, 2019-2020
Member	Executive Committee, Iowa Initiative for Artificial Intelligence (IIAI) The University of Iowa, 2019-2020
Member	Department Executive Committee Department of Computer Science, The University of Iowa, 2016-2019
Member	Faculty Recruitment Committee Department of Computer Science, The University of Iowa, 2015-2020
Mentor	Black Girls Do Science College of Engineering, The University of Iowa, 2015-2016
Mentor	Iowa Edge Classroom Experience Center for Diversity and Enrichment, The University of Iowa, 2015-2018
Mentor	Summer Research Opportunities Program (SROP) Graduate College, The University of Iowa, 2017
Mentor	Secondary Student Training Program (SSTP) Belin-Blank Center, The University of Iowa, 2016-2019

Patents

USPTO 10484881	Jia Wang, Lusheng Ji, Alex X. Liu, Zubair Shafiq. Optimization of cellular network architecture based on device type-specific traffic dynamics. November 2019
USPTO 10420167	Jia Wang, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Zubair Shafiq. Cellular Connection Sharing. September 2019

Expert Testimony & Reports

4:20-cv-05146	**Calhoun v. Google** District Court, N.D. California
4:21-cv-02155	**In re Google RTB Consumer Privacy Litigation** District Court, N.D. California
3:23-cv-02431	**Doe v. Google** District Court, N.D. California
22-01-88230-D	**State of Texas v. Google** District Court, Victoria County, Texas
A 2002633	**Doe v. Bon Secours Mercy Health** Court of Common Pleas, Hamilton County, Ohio
24-C-20-000591	**Doe v. Medstar Health** Circuit Court, Baltimore County, Maryland
19-2-26674-1	**Doe v. Virginia Mason** Superior Court, Washington
23CV037304	**Doe v. Family Planning Associates Medical Group** Superior Court, California
22-cv-03580	**In re Meta Pixel Healthcare Litigation** District Court, N.D. California
23OT01-0026	**Stake v. Knox** Court of Common Pleas, Knox County, Ohio

23-cv-00964	**Griffith v. TikTok** District Court, C.D. California
22STCV36304	**Doe v. Adventist** Superior Court, California
3:22-cv-07465	**Hazel v. Prudential** District Court, N.D. California
4:22-cv-04423	**Beke v. Fandom** District Court, N.D. California
3:22-cv-08981	**Lau v. Gen Digital** District Court, N.D. California
4:20-cv-00957	**State of Texas v. Google** District Court, E.D. Texas
2022-00859JD	**Caraway v. Wexner** Court of Claims, Ohio
2222-CC10014-01	**Doe v. SSM** Circuit Court of the City of St. Louis, Missouri
4:22-cv-05499	**Markels v. AARP** District Court, N.D. California

APPENDIX B

APPENDIX B: MATERIALS CONSIDERED

- Inspection of ActiveProspect Databases, Dec. 20, 2024
- Defendants' Motion for Summary Judgement and all attachments
- Wolfe Declaration in Support of Summary Judgment
- Polish Declaration in Support of Summary Judgment
- Prudential's Responses to Requests for Admission (set one)
- Defendants' Responses to Interrogatories (sets one thorugh four)
- Renz Deposition Transcript
- Rafferty Deposition Transcript
- Bao Deposition Transcript
- Wolfe Deposition Transcript
- Williams Deposition Transcript
- Polish Rough Deposition Transcript
- AP0000007
- AP0000039
- AP0000167
- AP0000169
- AP0000239
- AP0000388
- AP0000392
- AP0000394
- AP0000395
- AP0000483
- AP0000490
- AP0000492
- AP0000493
- AP0000494
- AP0000505
- AP0000506
- AP0000507
- AP0000509
- AP0000511
- AP0000512

- AP0000513
- AP0000514
- AP0000515
- AP0000516
- AP0000517
- AP0000518
- AP0000519
- AP0000574
- AP0000577
- AP0000585
- AP0000610
- AP0000628
- AP0000632
- AP0000674
- AP0000712
- AP0000720
- AP0000722
- AP0000729
- AP0000743
- AP0000747
- AP0000761
- AP0000768
- AP0000772
- AP0000847
- AP0000858
- AP0000865
- AP0000866
- AP0000867
- AP0000868
- AP0000869
- AP0000870
- AP0000872
- AP0000874

- AP0000876
- AP0000885
- AP0000887
- AP0000889
- AP0000896
- AP0000898
- AP0000900
- AP0000903
- AP0000905
- AP0000907
- AP0000908
- AP0000909
- AP0000910
- AP0000911
- AP0000912
- AP0000913
- AP0000914
- AP0000915
- AP0000916
- AP0000917
- AP0000918
- AP0000919
- AP0000920
- AP0000921
- AP0000922
- AP0000996
- AP0000997
- AP0000998
- AP0000999
- AP0001013
- AP0001015
- AP0001018
- AP0001020

- AP0001022
- AP0001024
- AP0001025
- AP0001026
- AP0001027
- AP0001028
- AP0001029
- AP0001030
- AP0001032
- PRU0000086
- PRU0000088
- PRU0000089
- PRU0000090
- PRU0000091
- PRU0000092
- PRU0000093
- PRU0000094
- PRU0000095
- PRU0000096
- PRU0000097
- PRU0002712
- PRU0002714
- PRU0005177
- PRU0005178
- PRU0005179
- PRU0005177
- PRU0005178
- PRU0005179
- Wolfe Dep. Ex. 142 (https://community.activeprospect.com/posts/4766190-trustedform-lead-matching)
- ActiveProspect Highly Confidential Source Code documents produced for inspection
    - AP_SCODE0000001-57
- term.prudential.com
    - term.prudential.com.har (accessed November 2023)

  - Internet Archive's Wayback Machine, (https://web.archive.org/web/20210401000000*/https://term.prudential.com/life)
  - Screen Recording.mov
- Translate TrustedForm Python Script
  - Translated Snapshot Payload
  - Translated Events Payload

- Amjad, A.H., Shafiq, Z. and Gulzar, M.A., 2023, January. *Blocking JavaScript without Breaking the Web*. In Privacy Enhancing Technologies Symposium (PETS).
- Acar, G., Englehardt, S. and Narayanan, A., 2020. *No boundaries: data exfiltration by third parties embedded on web pages*. Proceedings on Privacy Enhancing Technologies.
- Senol, A., Acar, G., Humbert, M. and Borgesius, F.Z., 2022. *Leaky forms: A study of email and password exfiltration before form submission*. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 1813-1830).
- bootstrap.js (https://cdn.trustedform.com/bootstrap.js?provide_referrer=false&field=xxTrustedFormCertUrl&l=17013362437130.2550676600214141&invert_field_sensitivity=false)
- trustedform-1.9.4.js (https://cdn.trustedform.com/trustedform-1.9.4.js)
- https://activeprospect.com/resources/discovering-trustedform-api/
- https://cdn.assurance.com/insurance/public/assets/trustedForm-4a1205758bed9df95ef0ff78d02f73edd84361c32de02c6addd014f63fde670a.js
- https://almanac.httparchive.org/en/2022/javascript
- https://cloud.google.com/security/products/recaptcha?hl=en
- https://developer.mozilla.org/en-US/docs/Glossary/Cookie
- https://developer.mozilla.org/en-US/docs/Glossary/Cryptographic_hash_function
- https://developer.mozilla.org/en-US/docs/Web/API/Document_Object_Model
- https://developer.mozilla.org/en-US/docs/Web/API/Document/scroll_event
- https://developer.mozilla.org/en-US/docs/Web/API/Element/click_event
- https://developer.mozilla.org/en-US/docs/Web/API/Element/keydown_event
- https://developer.mozilla.org/en-US/docs/Web/API/Event
- https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener.
- https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener#browser_compatibility
- https://developer.mozilla.org/en-US/docs/Web/API/MutationObserver
- https://developer.mozilla.org/en-US/docs/Web/API/MutationObserver#browser_compatibility
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cookie
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/POST

- https://developers.activeprospect.com/docs/trustedform/getting-started/
- https://docs.house.gov/meetings/IF/IF17/20180614/108413/HHRG-115-IF17-20180614-SD007.pdf
- https://gs.statcounter.com/browser-market-share/all/chart.php?device=Desktop%20%26%20Mobile%20%26%20Tablet%20%26%20Console&device_hidden=desktop%2Bmobile%2Btablet%2Bconsole&multi-device=true&statType_hidden=browser&region_hidden=US&granularity=monthly&statType=Browser&region=United%20States%20of%20America&fromInt=202304&toInt=202404&fromMonthYear=2023-04&toMonthYear=2024-04&csv=1
- https://innovation.ox.ac.uk/incubator-ventures/oxford-bio-chronometrics/
- https://oxford-biochron.com/
- https://trends.builtwith.com/analytics/Oxford-Biochronometrics
- https://trends.builtwith.com/widgets/reCAPTCHA
- https://webkit.org/tracking-prevention/#intelligent-tracking-prevention-itp
- https://www.cloudflare.com/learning/bots/what-is-a-bot/
- https://www.computerhope.com/issues/ch000891.htm
- https://www.google.com/recaptcha/about/
- https://www.google.com/recaptcha/intro/?zbcode=inc5000
- https://aws.amazon.com/dynamodb/
- https://aws.amazon.com/s3/
- https://aws.amazon.com/s3/storage-classes/glacier/
- https://cdn.trustedform.com/trustedform-1.9.4.js
- https://cloud.google.com/use-cases/ocr;
- https://developer.mozilla.org/en-US/docs/Web/API/KeyboardEvent/charCode
- https://developer.mozilla.org/en-US/docs/Web/API/KeyboardEvent/key
- https://developer.mozilla.org/en-US/docs/Web/API/KeyboardEvent/keyCode
- https://docs.aws.amazon.com/AmazonS3/latest/API/API_RestoreObject.html
- https://docs.aws.amazon.com/AmazonS3/latest/userguide/glacier-storage-classes.html
- https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects-retrieval-options.html
- https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/overview-ocr